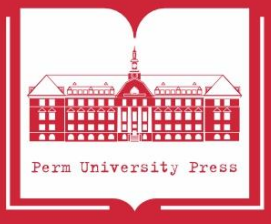
ПЕРМСКИЙ
ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Выпуск 1



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Сборник статей*

Выпуск 1


Пермь 2024

УДК 004
ББК 32.81
А437

А437 **Актуальные** проблемы информационной безопасности [Электронный ресурс] : сборник статей / Пермский государственный национальный исследовательский университет. – Электронные данные. – Пермь, 2024. – Вып. 1. – 3,64 Мб ; 143 с. – Режим доступа: http://www.psu.ru/files/docs/science/books/sborniki/aktualnye-problemy-informacionnoj-bezopasnosti-2024.pdf. – Заглавие с экрана.

ISBN 978-5-7944-4148-2

Сборник содержит статьи, посвященные различным проблемам информационной безопасности, являющимся наиболее актуальными в настоящее время в Российской Федерации. Данный выпуск сборника отражает результаты исследований по вопросам информационной безопасности, проводимых на различных предприятиях и в организациях Пермского края.

Материалы сборника предназначены для специалистов в области информационной безопасности.

**УДК 004**
**ББК 32.81**

*Издается по решению Института компьютерных наук и технологий Пермского государственного национального исследовательского университета*



*Рецензенты:* профессор кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, д-р техн. наук, доцент ***В. И. Фрейман***;

и.о. зав. кафедрой прикладной информатики, информационных систем и технологий, канд. техн. наук, д-р экон. наук, профессор ***Н. Л. Казаринова***;

д-р техн. наук, профессор ***О. Г. Пенский***

ISBN 978-5-7944-4148-2

# ОГЛАВЛЕНИЕ

# ПРЕДОТВРАЩЕНИЕ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ В ИНФОРМАЦИОННОЙ СРЕДЕ НА ЛЮДЕЙ ОТ 18 ДО 25 ЛЕТ

***И.В. Аникина, И.Г. Бузмаков, А.А. Бурылова, В.Ю. Кондратенков, У.И. Кузьминых, Е.Ю. Никитина, Т.С. Плахина, В.В. Полыгалов, А.В. Рычков, Д.А. Соболева***

Пермский государственный национальный исследовательский университет

**Аннотация**. В статье рассматриваются основные понятия деструктивного воздействия, как оно проявляется и какие последствия оно может иметь для граждан, стран и общества в целом, а также актуальность проблемы. Особое внимание уделяется использованию информационной сферы в качестве инструмента для деструктивного воздействия на молодежь. В статье представлен один из методов противодействия деструктивному воздействию, который включает в себя создание материалов, способствующих более критическому отношению к информации, научение выявлять дезинформацию и манипуляции, которые могут повлиять на поведение и мнения людей.

**Ключевые слова:** *котики, котики-патруль, деструктивное воздействие, информационная безопасность, информационное пространство, информационная среда, манипулирование общественным сознанием, психологические методы воздействия на человека, социальные сети*

Деструктивное воздействие на личность – это проблема, которая возникает в результате попытки оказать негативное воздействие на психологическое состояние и поведение человека. Такое воздействие может производиться различными способами: через словесное обращение, образы, звуки и цвета. Оно может быть направлено как на конкретного человека, так и на целые социальные группы.

В современном обществе, деструктивное воздействие на личность становится все более актуальной проблемой. Оно может привести к серьезным последствиям, таким как нарушение психического и физического здоровья человека, угроза безопасности и стабильности государства, экономические и политические потери [1].

Одним из наиболее эффективных способов деструктивного воздействия на личность является использование информационной сферы. Информационная сфера включает в себя все виды информации: от общественно-полезной до скандальной и противоречивой. Она также включает в себя все объекты информатизации, информационные системы, сайты, сети связи и информационные технологии, а также всех субъектов, занимающихся формированием и обработкой информации.

Для противодействия этой проблеме необходимо создать материалы, которые помогут людям стать более критичными и аналитическими в отношении

получаемой информации. Они должны уметь распознавать манипуляции и дезинформацию, анализировать ее и принимать информированные решения. Необходимо также создать систему защиты от деструктивного воздействия на личность, чтобы люди могли чувствовать себя более уверенно.

Одним из главных инструментов деструктивного воздействия является использование эмоционального фона, что позволяет убедительнее и эффективнее реализовать негативное влияние. Кроме того, использование ложной информации, фейковых новостей, спекуляций и других методов манипуляции становится все более распространенным.

Особую опасность представляет деструктивное воздействие на молодежь, которая является наиболее уязвимой к таким воздействиям. Молодежь, как правило, более открыта и восприимчива к новым идеям и мнениям, что может использоваться для их манипуляции. Кроме того, молодежь часто использует социальные сети и другие онлайн-платформы для получения информации, что делает их более подверженными дезинформации и манипуляции.

Для борьбы с деструктивным воздействием на личность необходимо принимать меры на разных уровнях: государственном, общественном и личном. На государственном уровне необходимо создавать законодательные механизмы для защиты граждан от дезинформации и манипуляции. На общественном уровне необходимо проводить образовательную работу и информировать население о методах деструктивного воздействия и способах защиты от него. На личном уровне необходимо учиться критически мыслить и анализировать информацию, а также не доверять всему, что говорится в СМИ и на Интернет-платформах.

В России существует несколько проектов, направленных на повышение знаний в области информационной безопасности среди молодежи. Некоторые из них:

1. Конкурс «Школа кибербезопасности» – ежегодный конкурс, организуемый Минцифры России совместно с Фондом развития информационной культуры. Цель конкурса – привлечение внимания школьников к вопросам кибербезопасности и развитие их компетенций в этой области.
2. Проект «Киберполигон» – это образовательная платформа, созданная Центром кибербезопасности Московского государственного университета имени М.В. Ломоносова. На платформе можно проходить онлайн-курсы, тренировки и тестирования по кибербезопасности.
3. Проект «Безопасный интернет» – инициатива, поддерживаемая Министерством образования РФ и Роскомнадзором. В рамках проекта проводятся семинары и тренинги для учащихся, а также публикуются материалы и рекомендации по безопасному поведению в интернете.

4. Программа «Информационная безопасность» – проект, проводимый в рамках социальной ответственности компании «Касперский». Программа включает в себя различные мероприятия для студентов и школьников, в том числе лекции, семинары, тренинги и конкурсы.

Формат данных аналогов недостаточно близок к интересам молодежи. В этих проектах информация преподносится на специфическом языке и может вызвать трудности для восприятия у людей, которые в своей повседневности не сталкиваются с данными темами.

С учетом вышесказанного было принято решение разработать новый проект, который будет преподносить информацию в более доступной и понятной форме для молодежи.

Целью данного проекта является повышение уровня осведомленности людей в вопросах информационной безопасности. Он направлен на противостояние деструктивному воздействию на людей в возрасте от 18 до 25 лет.

Проект реализован в форме интернет-ресурса, который будет содержать различные материалы на тему информационной безопасности, такие как статьи, видео, презентации и аудиозаписи. Контент будет подобран таким образом, чтобы каждый пользователь мог найти информацию по интересующей его теме. Не менее важным является то, что контент будет структурирован и преподноситься в легкой форме, что позволит пользователям быстро ознакомиться с необходимой информацией, не тратя много времени на чтение.

Исходя из возраста целевой аудитории, основной площадкой для распространения была выбрана социальная сеть «ВКонтакте», а именно публичное сообщество «Котики-патруль: информационная безопасность» (рис. 1, 2) [2]. Для привлечения и удержания внимания целевой аудитории было принято решение использовать в качестве особенности образы семейства кошачьих. Такой выбор был обоснован популярностью данных животных среди целевой аудитории.

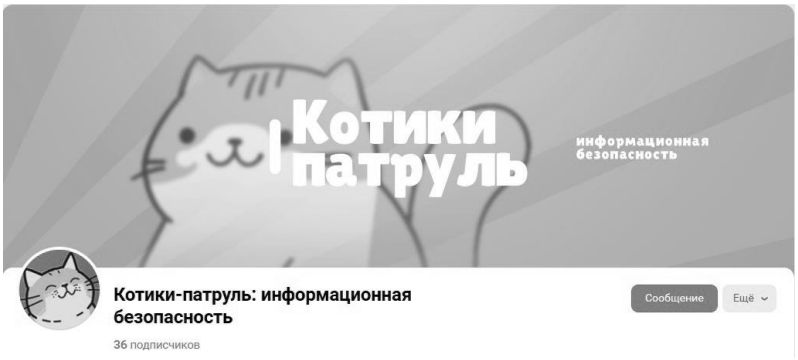



*Рис. 1. Шапка публичного сообщества*


*Рис. 2. Эмблема публичного сообщества*

Для проекта было принято решение о использовании модифицированной концепции «добра и зла» – модификация заключается в добавлении третьего действующего лица, находящегося на нейтральной стороне.

Данные персонажи используются в качестве иллюстративного представления информации, а также закрепления отличительной особенности реализуемого проекта от других похожих. В частности, персонажи используются как главные лица нарративов, описывающих некоторые случаи реализации деструктивного воздействия в информационной среде.

Были созданы 3 персонажа:

1. Антагонист;
2. Протагонист;
3. Обыватель.

В роли обывателя выступает персонаж по имени Зак (рис. 3). Он является котом, олицетворяющим среднестатистического человека, недостаточно осведомленного в области информационной безопасности. В связи с этим, он может поддаться деструктивному воздействию в информационной среде.

*Рис. 3. Изображение Зака*

В роли антагониста выступает персонаж по имени Шторм (рис. 4). Его главной целью является обман, кража и другие проявления деструктивного воздействия по отношению к Заку.

*Рис. 4. Изображение Шторма*

В роли протагониста выступает персонаж по имени Коди (рис. 5). Он является специалистом в области информационной безопасности, и его главной целью является защита Зака от деструктивного воздействия, которое оказывает на него Шторм.

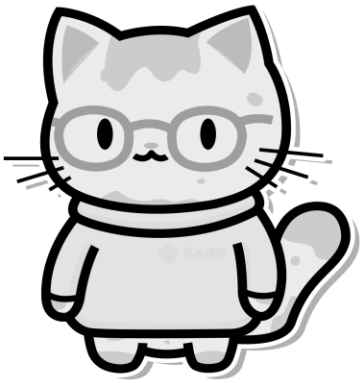


*Рис. 5. Изображение Коди*

Поскольку целевой аудиторией являются люди в возрасте 18–25 лет, основной акцент был сделан на неформальной атмосфере и соответствующей лексике.

Основным форматами представления информации были выбраны:

1. Развлекательные картинки, повествующие о проблемах в сфере информационной безопасности;

2. Статьи на тему информационной безопасности;

3. Истории с участием вышеперечисленных трех персонажей, описывающие один из сценариев возможного деструктивного воздействия в информационном пространстве;

4. Рубрика «Вопрос – Ответ»;

5. Опросы и инфографика на тему информационной безопасности и деструктивного воздействия;

6. Видеоролики, посвященные актуальным проблемам информационной безопасности;

7. Интервью со специалистами в области информационной безопасности;

8. Подборки книг, фильмов, сериалов на тему информационной безопасности.

Пробный запуск сообщества «Котики-патруль» в социальной сети «ВКонтакте» прошел успешно. Были получены положительные отзывы от подписчиков, которые высоко оценили представленный контент. На данный момент сообщество насчитывает всего 40 подписчиков. Такое количество подписавшихся обуславливается отсутствием рекламной кампании.

## Список литературы

1. Столяренко А.М., Сердюк Н.В., Вахнина В.В., Боева О.М., Грищенко Л.Л. Психологические аспекты деструктивного информационно-психологического воздействия [Электронный ресурс] // Психология и право. 2019. Том 9. № 4. С. 75–89. DOI: 10.17759/psylaw.2019090406

2. Публичное сообщество ВКонтакте «Котики-патруль: информационная безопасность» [Электронный ресурс] – URL: https://vk.com/kotiki_patrul (дата обращения 02.04.2023)

## PREVENTION OF DESTRUCTIVE INFLUENCE IN THE INFORMATIONAL ENVIRONMENT ON PEOPLE FROM 18 TO 25 YEARS OLD

***I.V. Anikina, I.G. Buzmakov, A.A. Burylova, V.Y. Kondratenkov, U.I. Kuzminikh, E.Yu. Nikitina, T.S. Plakhina, V.V. Polygalov, A.V. Rychkov, D.A. Soboleva***
Perm State National Research University

***Abstract.*** The article deals with the basic concepts of destructive influence, how it manifests itself and what consequences it can have for citizens, countries and society as a whole, as well as the relevance of the problem. Special attention is paid to the use of information sphere as a tool for destructive influence on youth. The article presents one of the methods of counteracting destructive influence, which includes the creation of materials that promote a more critical attitude to information, learning to identify misinformation and manipulation that can affect the behavior and opinions of people.

***Keywords:*** *cats, cats-patrol, destructive influence, information security, information space, information environment, manipulation of public consciousness, psychological methods of influencing a person, social networks.*

# ИССЛЕДОВАНИЕ РЕАЛИЗАЦИИ ПОТЕНЦИАЛА НАИБОЛЕЕ ВЛИЯТЕЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ

***П.В. Жданов, Я.Р. Мустакимова, А.Н. Рабчевский***

Пермский государственный национальный исследовательский университет,
ООО «Сеуслаб»

**Аннотация**. В статье рассматриваются наиболее влиятельные пользователи – это категория пользователей, чей потенциальный уровень влияния превышает уровень других пользователей данной социальной сети. Потенциальный уровень влияния (ПУВ) пользователя рассчитывается как произведение количества социальных связей этого пользователя (друзей и подписчиков) на количество публикаций пользователя. По сути, ПУВ пользователя соответствует максимально возможному количеству актов донесения его информации до других участников социальной сети. наличие высокого значения ПУВ соответствует лишь потенциальным возможностям влияния в сети, в то время как разные пользователи могут по-разному реализовывать свой потенциал влияния. Зная ПУВ и уровень его реализации можно более точно моделировать процессы распространения информации.

**Ключевые слова:** *пользователь, наиболее влиятельный пользователь, уровень влияния, распространение информации, влияние в сети, потенциал влияния.*

## Введение

Распространение информации в социальных сетях – это сложный процесс, включающий в себя множество людей и подверженный влиянию различных факторов. Одним из таких факторов является активность наиболее влиятельных пользователей.

Наиболее влиятельные пользователи – это категория пользователей, чей потенциальный уровень влияния превышает уровень других пользователей данной социальной сети. Потенциальный уровень влияния (ПУВ) пользователя рассчитывается как произведение количества социальных связей этого пользователя (друзей и подписчиков) на количество публикаций пользователя. По сути, ПУВ пользователя соответствует максимально возможному количеству актов донесения его информации до других участников социальной сети [1].

Согласно теории персонального маркетинга, распространение информации пользователями с высоким потенциалом влияния должно способствовать увеличению охвата аудитории. Посты таких пользователей должны получать много реакций в виде репостов, комментариев, лайков, и шире распространяться [2].

Однако, наличие высокого значения ПУВ соответствует лишь потенциальным возможностям влияния в сети, в то время как разные пользователи могут по-разному реализовывать свой потенциал влияния. Зная ПУВ и уровень

его реализации можно более точно моделировать процессы распространения информации.

Таким образом, актуальной является задача определения уровня реализации ПУВ пользователями в социальных сетях.

## Обзор литературы

Оценку реализации потенциального уровня влияния пользователя можно провести четырьмя методами [3]. Ими являются: оценка прямым сравнением, оценка с помощью ручных метрик, оценка через информационные треки и оценка через стохастические модели.

В первом методе используются оценки пользователей, полученные с использованием различных идентификационных алгоритмов, с показателями из социальных сетей: количество друзей и подписчиков пользователя, количество комментариев и того же контента, выложенного другими пользователями [4].

Во втором методе используются те же оценки пользователей, но они сравниваются с данными, полученными вручную, здесь важны используемые метрики и точность [5, 6].

В третьем методе используются треки распространения информации, строится их рейтинговый список, сравнивается с оценками пользователей, которые были получены различными идентификационными алгоритмами [7, 8].

В последнем методе используются стохастические модели, они включают в себя различные способы и моделируют ситуации путем учета случайных изменений входных данных [9].

Наиболее часто используется именно первый метод, так как данные в социальных сетях напрямую отражают как потенциальный уровень влияния пользователя, так и реализацию этого потенциала через различные показатели. Данный метод можно реализовать несколькими способами в зависимости от рассматриваемой социальной сети.

Одним из способов является построение двудольного графа. Такой метод был эффективен для социальной медиаплатформы YouTube, сам граф строился по комментариям [10]. Данный подход показал, что зависимость между влиятельностью пользователя и количеством оставленных комментариев не полная, то есть не всегда большая активность делает человека более влиятельным.

Способ, основанный на графах, также использовался в другом исследовании и основывался на социальной сети Pinterest [11]. Был использован двойной граф, чтобы оценить влияние пользователей социальной сети. Авторами статьи был сделан вывод, что влияние пользователей зависит как от структурных свойств социальной сети, так и от содержания контента, который публикуют пользователи социальной сети.

Другим способом является построение графика зависимости количества подписчиков от реализованного влияния [12], этот способ тестировался на социальной сети Twitter. В данном случае под реализованным влиянием понимается активность других пользователей на постах автора – лайки, комментарии и ретвиты. В данном исследовании было доказано, что при участии в различных информационных поводах у людей с меньшим количеством подписчиков может быть высокий уровень влияния. Информационный повод – это некоторое событие в общественной жизни или в социальной сети [13].

Рассматривая вопрос реализации потенциала, также есть исследования, утверждающие, что высокий потенциальный уровень влияния не имеет прямой корреляции с высоким уровнем его реализации. В одном из исследований говорится, что большое количество подписчиков не гарантирует успех и пользователи со средним количеством подписчиков могут быть более эффективны [14]. Также есть исследования, подтверждающие, что высокий показатель количества подписчиков может привести к более высокой симпатии, но при этом наиболее влиятельные пользователи не всегда автоматически воспринимаются как лидеры мнений [15].

Таким образом, не существует единого мнения насчет метода оценки реализации потенциального уровня влияния у наиболее влиятельных пользователей: согласно одним исследованиям, он должен быть наиболее высоким, согласно другим, наиболее высокая реализация данного потенциала может быть у совершенно разных пользователей.

## Постановка задачи

Необходимо было понять, действительно ли все наиболее влиятельные пользователи имеют большое влияние, и если нет, то от чего зависит уровень реализации их возможного влияния.

Для этого был использован метод оценки реализации ПУВ методом прямого сравнения: за величину ПУВ было взято произведение количества друзей рассматриваемого пользователя на его количество постов, а для оценки реализации потенциала влияния были рассмотрены реакции на посты данного пользователя. Под реакциями понимаются просмотры поста, репост поста, оставление комментариев под постом и лайки поста.

## Решение задачи

Было проведено исследование реализации потенциального уровня влияния на информационном поводе «Дворец Путина», который был направлен на понижение авторитета власти в государстве.

С помощью поисковой системы «SEUS»[1] была собрана коллекция постов по данному информационному поводу из социальной сети ВКонтакте. Из собранных данных были отобраны пользователи, значения ПУВ которых были наиболее высоки, то есть они являлись наиболее влиятельными пользователями для данного информационного повода. Далее были собраны суммарные количества просмотров, лайков, комментариев и репостов для всех постов по данной теме у каждого пользователя.

Теоретически, пользователи с большим ПУВ должны были иметь больше реакций на их посты. Ниже представлены графики, полученные в ходе анализа данных (рис. 1, рис. 2). На них представлена зависимость количества просмотров и репостов от ПУВ пользователя. Были взяты именно два этих показателя, так как график зависимости ПУВ от количества просмотров повторяет график лайков, но с большими амплитудами, и аналогичная ситуация происходит с графиком зависимости ПУВ от количества комментариев и репостов. Следует отметить, что зависимости между реакцией пользователей и значением ПУВ нет: ни прямой, ни экспоненциальной, просто случайные всплески на протяжении всего графика.

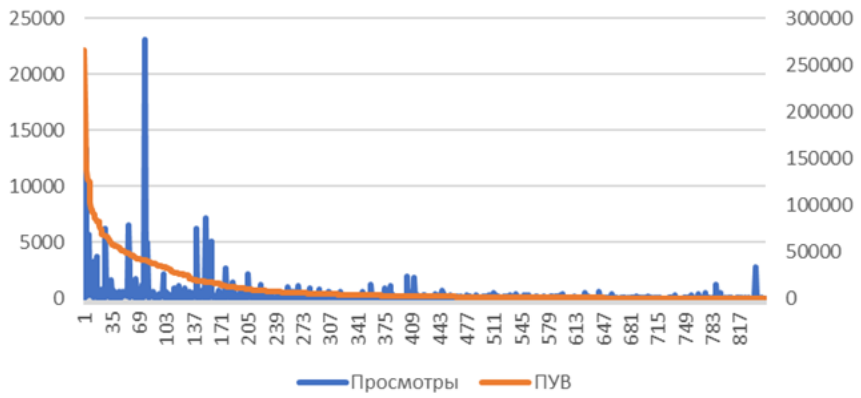



*Рис. 1. Зависимость количества просмотров от значения ПУВ*

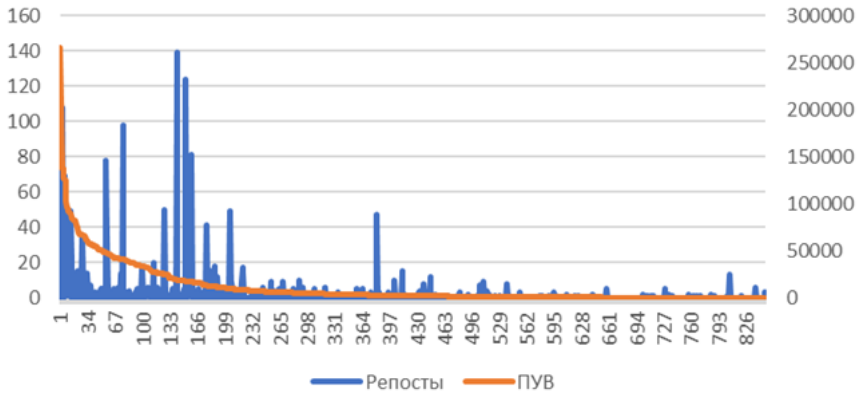



*Рис. 2. Зависимость количества репостов от значения ПУВ*

[1] SEUS – поисковая система информации в социальных сетях. Официальная страница сайта компании разработчика ООО «СЕУСЛАБ». URL: https://seuslab.ru/seus (дата обращения 12.12.2023 г.)

Рассматривая графики, в которых количество реакций на посты пользователя зависят от количества постов и количества друзей, можно прийти к выводу, что здесь тоже нет никакого рода зависимостей (рис. 3, рис. 4, рис. 5, рис. 6). Конечно, потенциал здесь все равно имеет значение. Если пользователи с более высокими значениями ПУВ все же его реализуют, то значения имеют тенденцию быть больше, чем у пользователей с невысоким ПУВ.


*Рис. 3. Зависимость количества просмотров от количества друзей*


*Рис. 4. Зависимость количества репостов от количества друзей*


*Рис. 5. Зависимость количества просмотров от количества постов*


*Рис. 6. Зависимость количества репостов от количества постов*

Из представленных выше графиков следует, что не все наиболее влиятельные пользователи реализуют свой потенциальный уровень влияния, участвуя в распространении информационного повода. Реализация ПУВ не зависит от количества друзей и количества постов, которые были выложены по данному информационному поводу.

Также было исследовано зависят ли друг от друга потенциальный уровень влияния и уровень реализации потенциала, который определяется как средняя сумма реакций на пост в отношении к потенциальному уровню влияния пользователя. Данная величина была графически соотнесена с величиной ПУВ (рис. 7). По графику видно, что с убыванием величины потенциального уровня влияния процент его реализации распределяется хаотично.


*Рис. 7. Отношение величины ПУВ к реализованному потенциалу*

Также было рассмотрено соотношение ПУВ и суммарной реакции, в которую входят просмотры, репосты, лайки (рис. 8). В целом, график, отображающий суммарную реакцию, некоторым образом повторяет график ПУВ. Но на графике видны выбросы. Эти выбросы необходимо исследовать дополнительно, чтобы понять, соответствуют они каким-то естественным событиям или нет.


*Рис. 8. Отношение величины ПУВ к суммарной реакции*

## Заключение

В ходе исследования было показано, что чем выше значения ПУВ, тем выше может быть абсолютное значение суммарной реакции и в среднем оно более высокое, чем у менее влиятельных пользователей, что само по себе нормально. Однако в результате более детального рассмотрения было обнаружено, что реализация потенциала влияния пользователя не зависит напрямую от самого значения ПУВ, от количества друзей или количества постов. То есть, если у пользователя есть большой потенциальный уровень влияния, то это не означает, что реакция на его посты также будет численно большой. Это объясняется тем, что каждый пользователь по-разному реализует свой потенциал влияния в сети.

Из чего можно сделать вывод, что реализация потенциала зависит от других параметров, а именно от самих людей, распространяющих информацию, от того, как они пишут свои посты, какие приемы используют в них, чтобы завладеть аудиторией и призвать её к действию или распространению определенной информации. Темой дальнейшего исследования должна быть попытка ответить на вопрос почему кто-то реализует свой потенциал, а кто-то нет, и за счет чего это происходит. Это может быть крайне полезно для того, чтобы прогнозировать процессы распространения информации во время информационных атак.

## Список литературы

1. Рабчевский А.Н., Рабчевский Е.А. Оценка потенциального уровня информационного влияния пользователей в социальных сетях // Информационные системы и технологии. 2022. №1(129). С. 114–122.

2. Qian W., Mao J. Exploring the Influential Factors of Personal Media Bloggers on Followers' Continuous Following Intention Based on Relationship Marketing Theory // *Behavioral Sciences.* 2023. V. 13(5).

3. Al-Garadi M., Varathan K., Ravana S., Ahmed E., Mujtaba G., Khan M., Khan S. Analysis of Online Social Network Connections for Identification of Influential Users: Survey and Open Research Issues // ACM Computing Surveys. 2018. V. 51.

4. Brown P., Feng J. Measuring user influence on twitter using modified k-shell decomposition // Proceedings of the International AAAI Conference on Web and Social Media. 2011. P. 18–23.

5. Chai W., Xu W., Zuo M., Wen X. ACQR: A novel framework to identify and predict influential users in microblogging // Proceedings of the Pacific Asia Conference on Information Systems. 2013.

6. Xiao C., Zhang Y., Zeng X., Wu Y. Predicting user influence in social media // Journal of Networks. 2013. V. 8(11). P. 2649– 2655.

7. Pei S., Muchnik L., Jr J., Zheng Z., Makse H. Searching for superspreaders of information in real-world social media // Scientific Reports. 2014. V. 4.

8. Ding Z., Jia Y., Zhou B., Han Y., He L., Zhang J. Measuring the spreadability of users in microblogs // Journal of Zhejiang University SCIENCE C. 2013. V. 14(9). P. 701–710.

9. Pei S., Muchnik L., Tang S., Zheng Z., Makse H. Exploring the complex pattern of information spreading in online blog communities // PloS one. 2015. V. 10(5).

10. Пастухов Р.К., Дробышевский М.Д., Турдаков Д.Ю. Определение влиятельных пользователей социальной сети по двудольному графу комментариев // Труды ИСП РАН. 2022. Т. 34. Вып. 5. С. 127-141.

11. Zhu Z., Su J., Kong L. Measuring influence in online social network based on the user-content bipartite graph // Computers in Human Behavior. 2015. V. 52. P. 184-189.

12. Fan C., Jiang Y., Mostafavi A. The Role of Local Influential Users in Spread of Situational Crisis Information // Journal of Computer-Mediated Communication. 2021. V. 26. I. 2. P. 108-127.

13. Рабчевский Е.А., Рабчевский А.Н. О некоторых аспектах структур пропаганды политического протеста в социальных сетях // Международное сотрудничество евразийских государств: политика, экономика, право. 2021. №1. С. 44-60.

14. What factors determine the effectiveness of social media influencers in promoting a brand or product? [Электронный ресурс] URL: https://edepot.wur.nl/513619 (дата обращения: 05.12.2023)

15. De Veirman M., Cauberghe V., Hudders L. Marketing through Instagram influencers: the impact of number of followers and product divergence on brand attitude // International Journal of Advertising. 2017. V. 36(5). P. 798–828.

## STUDY OF THE REALIZATION OF THE POTENTIAL OF THE MOST INFLUENTIAL USERS

***P.V. Zhdanov, Y.R. Mustakimova, A.N. Rabchevsky***
Perm State National Research University, LLC «Seuslab»

**Annotation.** The article considers the most influential users – a category of users whose potential level of influence exceeds the level of other users of a given social network. The potential influence level (MIU) of a user is calculated as the product of the number of social connections of this user (friends and subscribers) by the number of publications of the user. In fact, a user's MIU corresponds to the maximum possible number of acts of delivering his information to other participants of the social network. A high value of MIU corresponds only to potential opportunities of influence in the network, while different users can realize their potential for influence in different ways. Knowing the MIU and the level of its realization, it is possible to model the processes of information dissemination more accurately.
**Keywords:** *user, most influential user, level of influence, information dissemination, influence in the network, influence potential.*

## ВЛИЯНИЕ ЗАКОНОВ РОБОТОТЕХНИКИ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РОБОТОВ

***Г.О. Иванов***
Пермский национальный исследовательский политехнический университет

**Аннотация**. Законы робототехники были созданы чтобы обезопасить человека от потенциально опасных действий робота, обладающего искусственным интеллектом со способностью к мышлению. Но идеальная модель такого робота еще не создана, ввиду чего законы на практике реализуются лишь частично. Этого удалось достичь за счет значительного продвижения в области обучения искусственного интеллекта. Тенденция показывает, что роботы постепенно приближаются к обретению упрощенного создания, что позволит в полной мере реализовать законы робототехники. Это приводит к появлению проблемы обеспечения информационной безопасности, поскольку, роботы рассматриваются с точки зрения объекта, а наличие сознания делает их субъектами. В данной статье формулируется проблема влияния двойственности восприятия объекта-субъекта на информационную безопасность робота и выдвигается гипотеза по ее решению.
**Ключевые слова:** *робот; законы робототехники; практическое применение; информационная безопасность*

## Введение

Законы робототехники возникли на основе научно-фантастических рассказов писателя Айзека Азимова. Всего было сформулировано три закона:

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред;

2. Робот должен повиноваться всем приказам, которые дает человек, кроме тех случаев, когда эти приказы противоречат Первому Закону;

3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму Законам. [1]

Законы представляют из себя набор правил, которым неукоснительно должен следовать робот, обладающий искусственным интеллектом. Их смысл заключается в том, чтобы обезопасить жизнь человека и целостность робота от возникновения опасных ситуаций, которые могут быть спровоцированы искусственным интеллектом.

С учетом нынешней тенденции, когда роботы смогли войти в повседневную жизнь и больше не вызывают у людей страха «выйти из строя и уничтожить все человечество», профессор Фрэнк Паскуале предложил дополнение к законам Азимова в виде четырех новых пунктов:

1. Цифровые технологии должны дополнять профессионалов, а не заменять их;

2. Искусственный интеллект и роботизированные системы не должны подделывать человека;

3. В области искусственного интеллекта следует предотвратить усиление гонок вооружения с нулевой суммой;

4. Роботы и системы искусственного интеллекта должны указывать на личность своих создателей, контролирующих их людей и владельцев. [2]

По мнению Паскуале, человека необходимо защищать не только от прямого негативного воздействия роботов, но и от косвенного, когда искусственный интеллект становится инструментом в гонке вооружений или может стать причиной, по которой человек потеряет свое место в обществе. [3]

Законы Азимова и дополнение Паскуале создавались под идеальную модель – искусственный интеллект со способностью мыслить, что приравнивало бы его к человеку. Но такую модель можно считать идеальной и на сегодняшний день она не существует. Однако, технологии обучения искусственного интеллекта продвинулись настолько далеко, что действия роботов все точнее и точнее имитируют поведение человека. С учетом этого, можно допустить, что в определенных системах становится возможным создание робота с упрощенной способностью мыслить. Несмотря на то, что для этого потребуется ввести мно-

жество ограничений, тем не менее, для такого робота становится возможным на практике реализовать все законы робототехники. Как было сказано ранее, эти законы позволят обезопасить жизнь человека и целостность робота, но с другой стороны, они приведут к появлению новых факторов, которые будут оказывать влияние на безопасность информационной системы робота. [4]

**Восприятие роботов как объекта и субъекта**

В вопросе информационной безопасности простые модели роботов приравниваются к активам, то есть это объекты, которые владелец (субъект) хочет защитить от неправомерного доступа. Зачастую, такие модели способны выполнять ограниченный функционал, например, совершать манипуляции в пространстве. Более продвинутые модели способны объединять в себе множество различных функций и работать практически автономно. Они создаются с учетом аспектов информационной безопасности, то есть их архитектура включает в себя встроенные модули защиты, поэтому, их можно отнести к автоматизированным системам. С другой стороны, роботы к которым становятся применимы законы робототехники приравниваются к субъектам, поскольку, они обладают способностью вести себя как человек [5–7]. Но для обеспечения конфиденциальности, целостности и доступности информации необходимо однозначно определить кем является робот: объектом или субъектом защиты.

Необходимость возникает ввиду того, что объект и субъект требуют разного подхода с точки зрения защиты информации. Объект или актив требует защиты, чтобы только легитимный субъект или пользователь мог получить к нему доступ [8]. Для решения этой задачи традиционно могут применяться программно-аппаратные средства криптографической защиты, резервного копирования, сервер имен и так далее. В свою очередь субъекту или пользователю требуется защита от некорректного использования доступа к объекту и атак по типу социальной инженерии. Для этого, например, пользователя обучают как правильно взаимодействовать с активом и не попадаться на фишинговые атаки. Не будем также забывать и о стандартном представлении пары субъект-объект, где первым является человек, а вторым – вещь. Это позволяет понять, что методы и средства, применяемые для защиты одного, зачастую, не могут быть применены для защиты другого. В случае же с роботом, появляется двойственность (рис. 1), при которой в одном лице существует и объект, и субъект. [9]

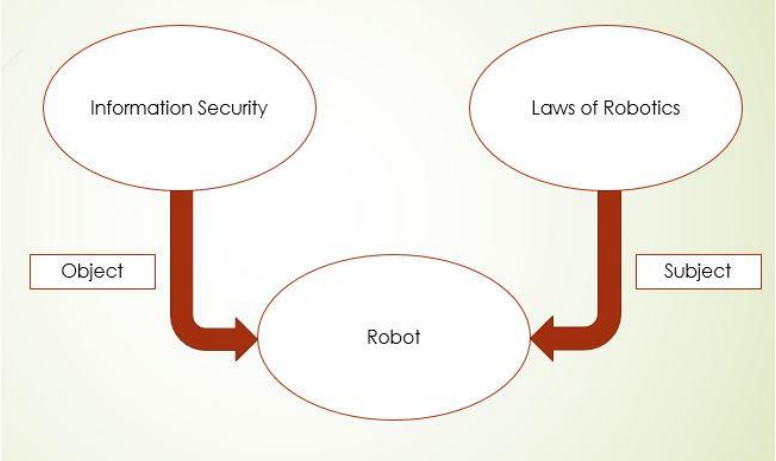



*Рис. 1. Двойственное восприятие робота*

Для понимания проблемы наличия робота субъекта-объекта, в качестве аналогии разберем ситуацию, если бы в полностью автономную и защищенную автоматизированную систему посадили за управление администратора с нулевым уровнем знаний. Как итог, уровень защищенности значительно снизится, так как появятся новые уязвимости, реализуемые с помощью атак по типу социальная инженерия или в результате действий некомпетентного администратора. А поскольку, ранее, эта была полностью автономная система, соответственно, от этих уязвимостей защита не была предусмотрена, и система более не сможет считаться защищенной. Также, следует учитывать, что защите системы предпочтение будет отдаваться не нанесению вреда человеку, в соответствии с законами робототехники. Как итог, это начнет оказывать влияние на выбор действий администратора системы, заставляя его намеренно совершать выбор не в пользу обеспечения информационной безопасности системы.

Какие в таком случае возникают проблемы обеспечения информационной безопасность роботов при реализации законов робототехники?

## Проблема и решение

В первую очередь роботы субъект-объекты становятся новой категорией, для которых действующие стандартны по информационной безопасности, опирающиеся только на понятия субъект и объект, станут неактуальны. Это означает, что уровень защищенности такой системы будет определяться только разработчиком, давая ему право установить свою монополию, которая может быть ничем не обоснована.

Следуя законам робототехники, робот может стать источником информационной угрозой сам для себя. Наличие приоритета не нанесения вреда человеку над собственной безопасностью означает, что робот может допустить реализацию нарушения конфиденциальности, целостности, доступности информа-

ции, если в противном случае его действия будут создавать угрозу человеку. Это не исключает и того, что в результате применения контрмер роботом может пострадать и сам злоумышленник, совершающий атаку, таким образом, создавая новый тип атаки: шантаж угрозой нанесения себе вреда, в случае применения роботом защитных контрмер.

Неукоснительное следование законам робототехники предрасполагает к появлению новых типов атак, которые будут затрагивать моральные аспекты выбора и перетекать в социальную инженерию. Если раньше злоумышленникам приходилось иметь дело с бездушной машиной и искать дыры в программном коде, то теперь эту же машину можно попытаться обмануть как человека [10].

Одновременно выполняя рекомендации по защите и субъекта, и объекта, между методами и средствами может возникать ранее неизвестная синергия. Это может привести к тому, что исказится их реальное влияние на уровень защищенности системы, а также могут появиться новые уязвимости и вектора атаки на систему.

Как с этими проблемами можно бороться? Ответа на этот вопрос еще нет, но можно предположить в каких направлениях следует двигаться чтобы снизить негативное влияние применения законов робототехники на информационную безопасность роботов:

1. Дополнить модель CIA новыми параметрами. Это может позволить учесть особенности обмена информации в роботах субъектах-объектах и сделать действующие стандартны по защите информации применимыми, возможно, с внесением незначительных изменений или добавления новых категорий;

2. Ввести понятие субъект-объект. Это позволит на более основательном уровне пересмотреть связь понятий и заложить основу для создания отраслевых стандартов для роботов, а также применить лучшие практики из действующих стандартов, базирующихся только на понятиях субъект и объект;

3. Разграничить сферу применения. Если роботы с искусственным интеллектом, обладающие сознанием и следующие законам робототехники будут классифицированы и отнесены к понятию субъект как человек, то задача сведется к поиску перехода такого робота от класса объект к субъекту. Также следует учитывать, что при становлении субъектом эти роботы будут ограничены тем же функционалом влияния на информационную систему, что и люди. В противном случае потребуется проводить более глубокое классифицирование и определять степени влияния роботов-субъектов на информационные системы.

## Заключение

Подводя итоги, стоит отметить, что сегодняшние роботы с искусственным интеллектом могут казаться далекими от приобретения упрощенного мышления, но технологии и методы меняются, а законы переписываются. Возможно, уже завтра мы столкнемся с прорывной технологии в области обучения роботов, а может быть законы робототехники будут переписаны и в информационной безопасности появится понятие двойственного объекта-субъекта. Важно учитывать стремительные темпы роста робототехнической области и быть готовыми адаптироваться к будущим проблемам.

## Список литературы


1. Как работают три закона робототехники Айзека Азимова и зачем их придумали? // [Электронный ресурс] Режим доступа: https://habr.com/ru/company/skillfactory/blog/528236/ (дата обращения: 19.10.2022).

2. Три закона Азимова помогли сформировать ИИ. Нам нужно еще четыре // [Электронный ресурс] – Режим доступа: https://asimovonline.ru/zakony-robototekhniki/ (дата обращения: 20.10.2022).

3. Gogu, G., Ray, P., Neagoe, M., Gogu, G., Diaconescu, D., Pocola, A.G., Pop, D.O., Petra, C.: Robotics and manufacturing. In: Talaba, D., Roche, T. (eds.) // Product Engineering: Eco-Design, Technologies and Green Energy, p. 348. Springer, Cham (2006).

4. Jean-Paul A. Yaacoub, H. Noura, O. Salman, A. Chehab. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations // Springer – 2021.

5. Fanuc. The factory automation company // [Электронный ресурс] – Режим доступа: https://academy-sp.fanuc.eu (дата обращения: 06.06.2022).

6. A. Santos, A. Cunha, and N. Macedo. Property-based testing for the robot operating system // In Proceedings of the 9th ACM SIGSOFT International Workshop on Automating TEST Case Design, pages 56–62, 2018.

7. V.M. Vilches, L.A. Kirschgens, A.B. Calvo, A.H. Cordero, R.I. Pisón, D.M. Vilches, A.M. Rosas, G.O. Mendia, L.U.S. Juan, I.Z. Ugarte, et al. Introducing the robot security framework (rsf), a standardized methodology to perform security assessments in robotics // arXiv preprint arXiv:1806.04042, 2018.

8. Nicholas DeMarinis, Stefanie Tellex, Vasileios Kemerlis, George Konidaris, Rodrigo Fonseca. Scanning the Internet for ROS: A View of Security in Robotics Research // IEEE – 2019.

9. Beasley R.A.: Medical robots: current systems and research // J. Robot. (2012).

10. Cheein F.A.A., Carelli, R.: Agricultural robotics: unmanned robotic service units in agricultural tasks // IEEE Ind. Electron. Mag. 7(3), 48–58 (2013).

## INFLUENCE OF ROBOTICS LAWS ON INFORMATION SECURITY OF ROBOTS

***G.O. Ivanov***

Perm National Research Polytechnic University

**Abstract.** The laws of robotics were created to protect humans from potentially dangerous actions of a robot possessing artificial intelligence with the ability to think. But the ideal model of such a robot has not been created yet, so the laws are only partially realized in practice. This has been achieved by significant advances in the field of artificial intelligence training. The trend shows that robots are gradually approaching a simplified creation that will allow the laws of robotics to be fully realized. This leads to the problem of information security, because robots are considered from the point of view of an object, and the presence of consciousness makes them subjects. In this paper the problem of influence of duality of object-subject perception on information security of robot is formulated and hypothesis on its solution is put forward.

**Keywords:** *robot; laws of robotics; practical application; information security*

## ЦИФРОВАЯ ОБРАЗОВАТЕЛЬНАЯ ПЛАТФОРМА ПО ЗАЩИТЕ ИНФОРМАЦИИ

***Д.Е. Ильченко, В.В. Михалев, П.В. Шульгин***

Пермский военный институт войск национальной гвардии Российской Федерации

**Аннотация.** В статье обсуждаются вопросы тенденций информационной безопасности (ИБ), необходимость разработки цифровой платформы по защите информации, предъявляемые к ней требования. Структура разработанной платформы и ее дальнейшие перспективы развития. Результаты работы могут быть использованы военнослужащими и специалистами в области информационных технологий (ИТ) в отдельном ведомственном сегменте сети.

**Ключевые слова:** *цифровая платформа, защита информации, тенденции информационной безопасности*.

### Введение

На протяжении последних лет наблюдается устойчивый рост и сложность киберугроз, которые представляют серьёзные вызовы для нас всех. На ряду с развитием современных ИТ и цифровизацией нашей жизни, кибербезопасность становиться все более актуальной проблемой. В 2024 году, судя по текущим тенденциям, ожидается увеличение масштаба и динамики атак, так же как и их сложности. Киберпреступники становятся все более искусными в своих дей-

ствиях, используя новейшие технологии и методы для нарушения безопасности информации.

Говоря о новых угрозах, хотелось бы затронуть современные тенденции нынешнего и следующего года.

1. Ransomware – тип зловредного ПО, предназначенный для вымогательства. Он блокирует доступ компьютерной системе или предотвращает считывание записанных в нем данных, а затем требует от жертвы выкуп за восстановление исходного состояния. Ожидается увеличение количества атак и усложнение инструментария.

2. IoT – количество устройств IoT продолжает расти. Киберпреступники используют устройства IoT для атак на сети организаций и системы умных домов. Существуют уязвимости за счет генерирования устройствами Интернета вещей большого объема данных, риск взлома технологий, использование злоумышленниками подключенных устройств для прослушивания домов пользователей, сбор личной информации о человеке.

3. Социальная инженерия – киберпреступники будут активно пользоваться методами социальной инженерии, которая становится все более изощренной и сложной для обнаружения. Хотя специалисты по информационной безопасности и добились больших успехов в защите от традиционных кибератак, атаки с применением социальной инженерии продолжают ускользать даже от самых современных систем безопасности.

4. Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности. Является наиболее распространенной угрозой, и в 2024 году ожидается, что она все также будет использоваться для получения доступа к данным пользователей.

5. Криптовалютные атаки – количество атак, направленных на уязвимость криптовалютных бирж, увеличивается с течением времени: слишком большое вознаграждение стоит за атакой. К сожалению, ведущие компании в области кибербезопасности только присматриваются к новой картине атак, а создатели криптобирж пока пренебрегают безопасностью в угоду быстрой прибыли.

6. Угрозы, связанные с искусственным интеллектом (ИИ) – чтобы провести атаку на ИИ, злоумышленник получает доступ к обучающей выборке и добавляет в выборку объекты с неправильной разметкой. Обученная на искажённой выборке, модель будет ошибаться и на других схожих объектах.

На рис. 1 показана статистика за 2022 год по способам распространения шпионского ПО в успешных атаках на частные лица.

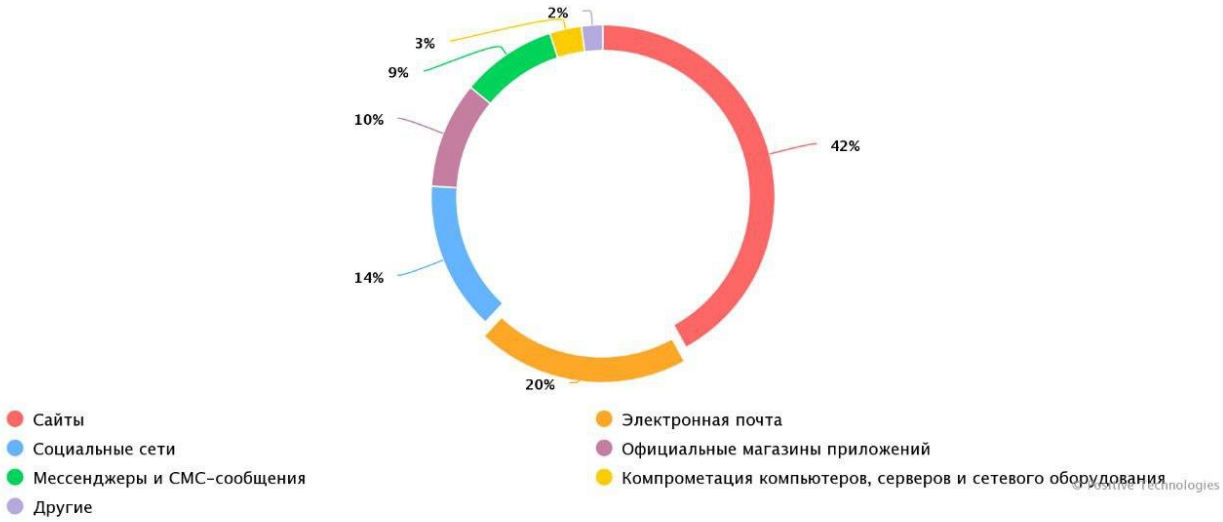



*Рис. 1. Способы распространения шпионского ПО в успешных атаках на частные лица*

Видно, что большая доля распространения ПО в успешных атаках приходится на сайты, электронные почты и социальные сети.

Одной из основных причин, связанных с развитием векторов атак, является низкая информационная грамотность и понимание технологий безопасности.

**Цель работы.** Разработать цифровую образовательную платформу по защите информации для обучения и повышения квалификации военнослужащих и специалистов в области ИТ в отдельном ведомственном сегменте сети.

Платформа предоставит инструменты для распространения знаний в области защиты информации, предоставляя пользователям материалы для организации ее защиты, а также доступным методам предотвращения кибератак, оставаясь вне зависимости от локации и времени.

**Требования к цифровой образовательной платформе.**

Исходя из цели к платформе были выдвинуты следующие требования:

1. Платформа должна быть клиент серверной;
2. Доступ к платформе должен осуществляться через WEB-интерфейс компьютера, подключенного к внутренней сети;
3. Платформа должна обеспечивать разграничение прав для различных категорий пользователей;
4. Платформа должна подходить под различные категории военнослужащих;
5. Платформа должна предоставлять ресурсы для самостоятельного изучения дисциплин под конкретные нужды обучающегося;
6. Платформа должна содержать разнообразные образовательные ресурсы: методические материалы, включая учебную литературу, видеоматериалы и тесты;

7. Должна быть реализована панель администратора для управления пользователями и контентом на страницах.

**Разработка цифровой образовательной платформы по защите информации**

Платформа, представленная на рисунке 2, разрабатывается для специалистов ИТ и военнослужащих войск национальной гвардии в отдельном ведомственном сегменте сети, однако наполнение разделов и сами разделы можно изменить при помощи панели администратора, для перестройки под различные организации.

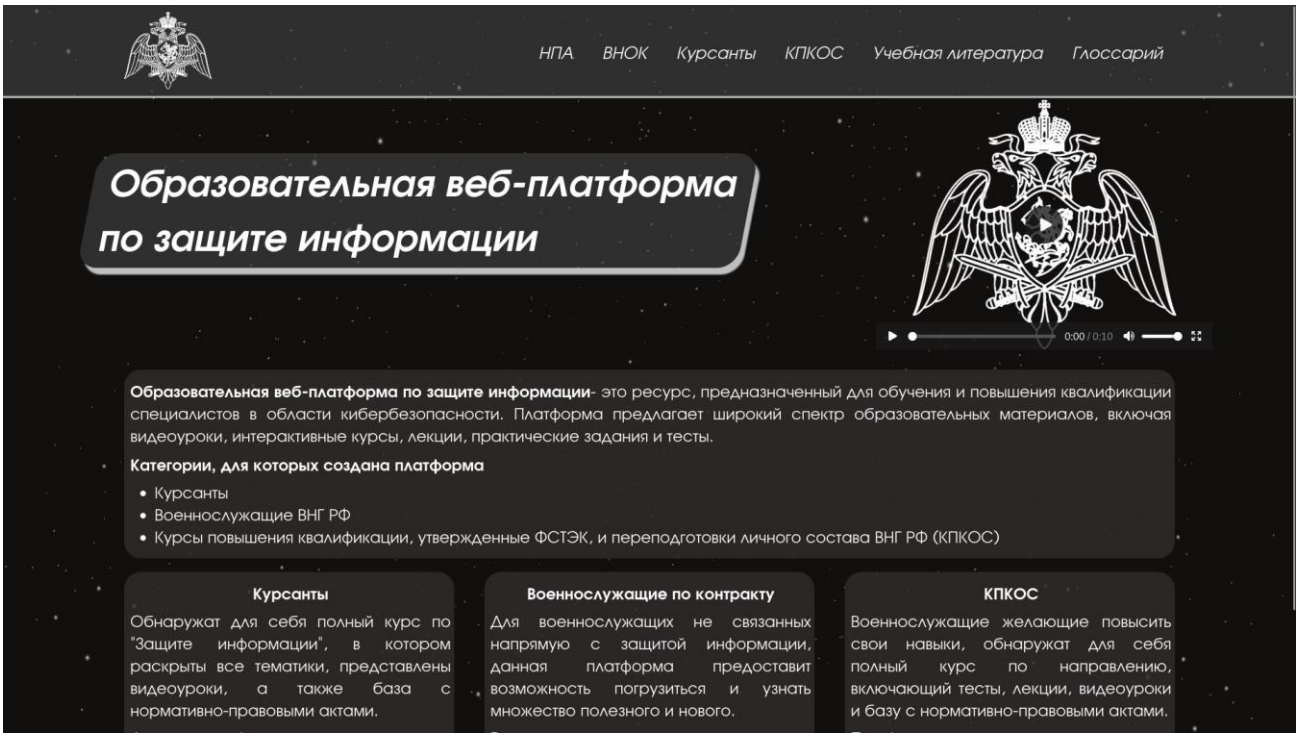



*Рис. 2. Разрабатываемая платформа*

Платформа предлагает широкий спектр возможностей и ресурсов для эффективного обучения. Она включает различные разделы, такие как:

1. «Нормативные правовые акты» (НПА) с необходимой правовой базой в области защиты информации;

2. «Военно-научное общество курсантов» (ВНОК), включающий в себя следующие подразделы: «Рационализаторские предложения», «Форумы разработчиков», «Рефераты», «Конференции», «Статьи» и «Выпускные квалификационные работы»;

3. «Курсанты» с подразделами «Основы информационной безопасности», «Методические материалы» с разделением на «Техническая защита информации» и «Информационная безопасность», «Видеоматериалы», а также «Нормативно-правовые акты».

4. «Курсы повышения квалификации офицерского состава» (КПКОС) с подразделами по направлениям повышения квалификации и переподготовки.

5. «Учебная литература» – различные учебные пособия и лабораторные практикумы по защите информации.

6. «Глоссарий» – словарь узкоспециализированных терминов по разделам дисциплин.

Каждое занятие платформы, представленное на рисунке 3, включает в себя название темы, занятия, учебные вопросы, используемую на занятии литературу, теоретический материал, презентационный материал, а также тестовое задание на основе пройденного материала для самопроверки – рисунок 4.

Особенно важным является наличие практических заданий, которые помогают студентам применить полученные знания на практике и убедиться в их эффективности.

Видеоматериал, в свою очередь, делает обучение более доступным и наглядным, что способствует более глубокому усвоению материала.

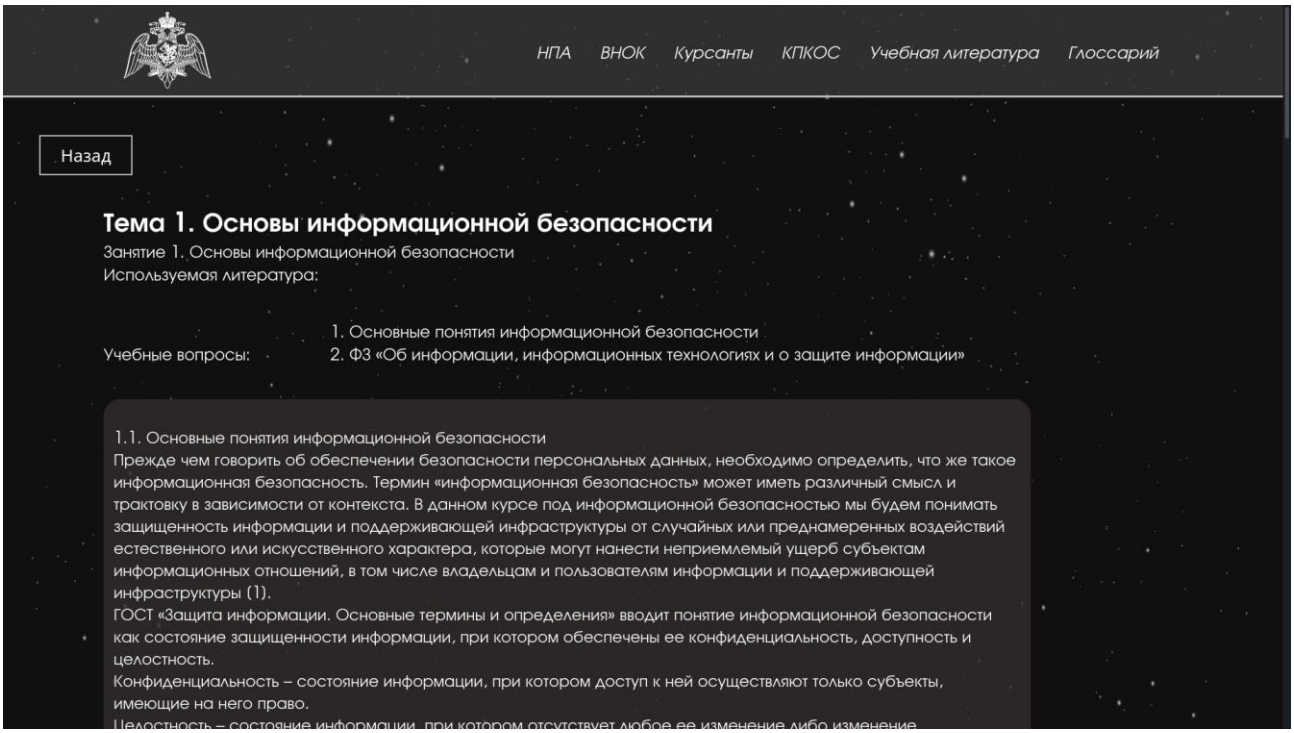



*Рис. 3. Занятие раздела «Основы информационной безопасности»*

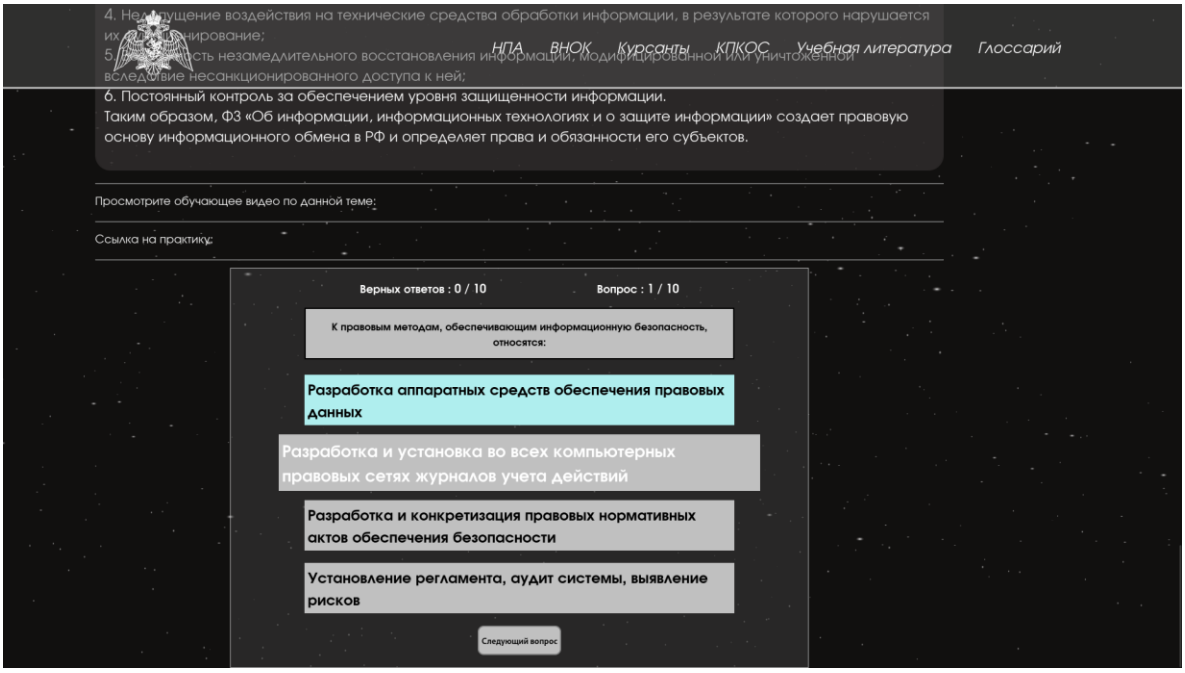



*Рис. 4. Тестовое задание на основе пройденного материала*

Управление платформой осуществляется через встроенную панель администратора, доступ к которой осуществляется через WEB-интерфейс, представленный на рис. 5.

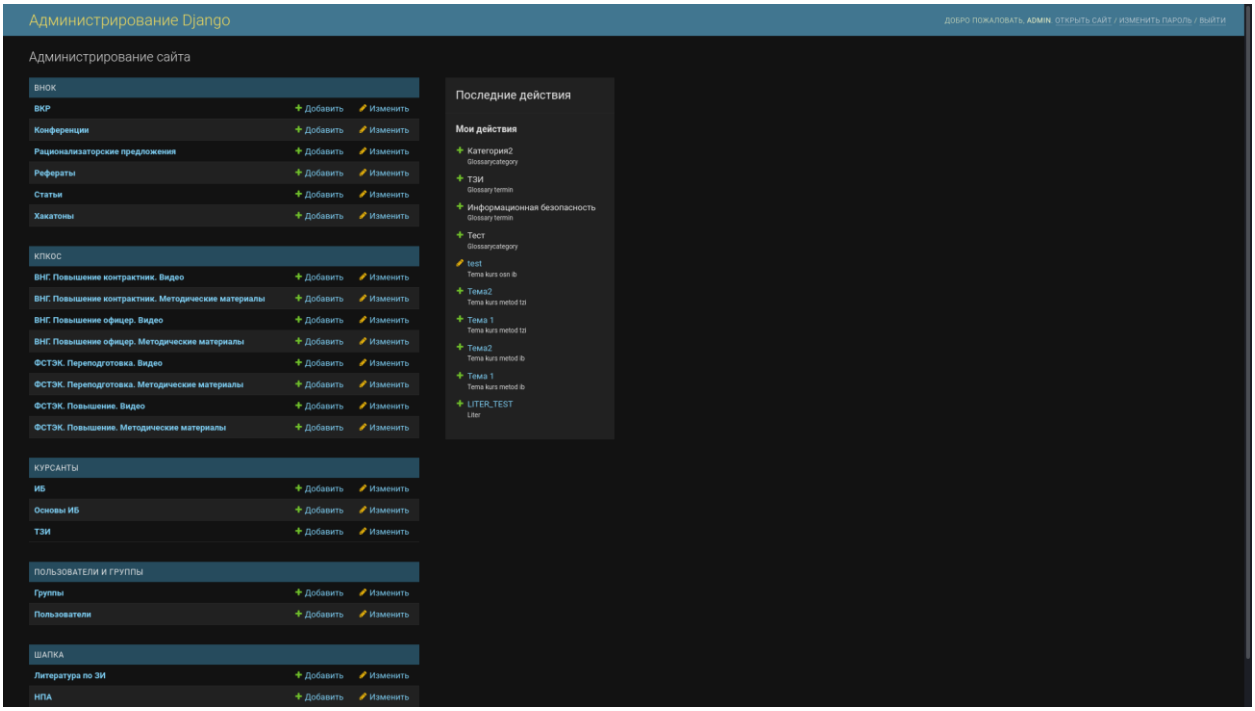



*Рис. 5. Панель администрирования платформы*

В рамках развития платформы планируется:

1. Создание автономного модуля для тестирования, с возможностью загрузки подготовленного в тестовом редакторе файла с тестом и отслеживания набранных баллов авторизованных пользователей;

2. Дополнение всех разделов контентом.

## Заключение

Таким образом, подчеркивается важность разработки цифровой образовательной платформы по защите информации в нашем быстро развивающемся мире. Разнообразие курсов, видеоматериалов, практических заданий и тестов предоставляет возможность углубленного изучения защиты информации.

Платформа обеспечивает обучающимся доступ к актуальным знаниям, гибкость в обучении, что делает ее важным инструментом для личного и профессионального развития военнослужащих и специалистов в области ИТ.

## Список литературы

1. В.В. Гафнер. Информационная безопасность: учебное пособие в 2 ч. / В.В. Гафнер ; ГОУ ВПО «Урал. Гос. Пед. Ун-т». – Екатеринбург, 2009. – Ч.1. – 155 с. – ISBN 978-5-7186-0414-6

2. В.А. Дронов. Django 4. Практика создания веб-сайтов на Python / В.А. Дронов; СПб.: БХВ-Петербург, 2021 – 672 с. – ISBN 978-5-9775-4058-2

# DIGITAL EDUCATIONAL PLATFORM FOR INFORMATION PROTECTION

***D.E. Ilchenko, V.V. Mikhalev, P.V. Shulgin***

Perm Military Institute of National Guard Forces of the Russian Federation

**Abstract.** The article discusses the issues of information security (IS) trends, the necessity to develop a digital platform for information protection, and the requirements to it. The structure of the developed platform and its further development prospects. The results of the work can be used by military personnel and specialists in the field of information technologies (IT) in a separate departmental segment of the network.

**Keywords:** *digital platform, information protection, information security trends.*

# РАЗРАБОТКА МОДЕЛИ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ОРГАНИЗАЦИОННЫХ МЕР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АССН С ИСПОЛЬЗОВАНИЕМ РЕГРЕССИОННОГО АНАЛИЗА

***Н.С. Кобяков***
Пермский военный институт войск национальной гвардии
Российской Федерации

**Аннотация.** В статье обсуждаются вопросы оценки эффективности организационных мер обеспечения информационной безопасности, направленные на подготовку пользователей автоматизированных систем специального назначения. Для формирования модели применяется регрессионный анализ. Результаты работы могут быть использованы должностными лицами, ответственными за обеспечение информационной безопасности для подготовки пользователей к эксплуатации автоматизированных систем в условиях реализации деструктивных функций неизвестных вредоносных программ.
**Ключевые слова:** *информационная безопасность, автоматизированная система, вредоносные программы*.

## Введение

В условиях постоянно совершенствующихся методов реализации деструктивных воздействий на автоматизированные системы специального назначения. Согласно [1] одной из наиболее актуальных угроз является внедрение вредоносного программного обеспечения. В работах [2-4] определена классификация вредоносных программ, актуальных для автоматизированных систем специального назначения:

1. Вредоносные утилиты.
2. Троянские программы.
3. Вирусы и черви.

Также, в данных работах определены модели для оценки опасности их деструктивного воздействия на автоматизированных системы специального назначения. Порядок реализации организационных мер определен в работе [5]. Согласно данного подхода в зависимости от опасности вредоносной программы определяется набор мер, необходимый для обеспечения информационной безопасности.

**Цель работы.** Разработать модель для оценки эффективности организационных мер обеспечения информационной безопасности, направленные на подготовку пользователей автоматизированных систем специального назначе-

ния в условиях реализации деструктивных функций неизвестных вредоносных программ с использованием регрессионного анализа.

**Постановка задачи.**

Для достижения цели работы необходимо решить следующие задачи:

1. Определить исходные данные для формирования модели.

2. Провести опрос высококвалифицированных специалистов, обеспечивающих информационную безопасность в результате сформировать обучающий и тестовый набор данных.

3. Сформировать модель для оценки эффективности организационных мер с использованием пакета прикладных программ.

4. Выполнить верификацию модели на тестовом наборе данных.

**Определение исходных данных для формирования модели**

Для формирования модели оценки эффективности организационных мер необходимо определить цели, достигаемые при их реализации. Опыт обеспечения информационной безопасности автоматизированных систем и результаты работ [6,7] подтверждают, что организационные меры проводятся для:

1. Недопущение создания угроз реализации деструктивных функций вредоносных программ при эксплуатации автоматизированных систем специального назначения ($m_1$).

2. Умение пользователей эксплуатировать автоматизированную систему специального назначения в условиях реализации деструктивных функций неизвестных вредоносных программ ($m_2$).

3. Знание и понимание алгоритма действий в случае обнаружения признаков реализации деструктивных функций вредоносных программ на автоматизированном рабочем месте пользователя ($m_3$).

4. Понимание ответственности за нарушение новых требований по обеспечению безопасности информации, обрабатываемой в автоматизированной системе специального назначения ($m_4$).

5. Осведомленность пользователей о появлении неизвестной вредоносной программы ($m_5$).

Достижение всех целей позволит значительно снизить вероятность реализации деструктивных функций вредоносных программ и снизить ущерб, в случае реализации. Но, вместе с тем, реализация мер, в ходе которых будут достигнуты все цели может занять очень много времени у должностных лиц ответственных за обеспечение информационной безопасности и пользователей. Следовательно, принятые меры должны соответствовать уровню опасности вредоносной программы.

Для оценки эффективности организационных мер обеспечения информационной безопасности целесообразно использовать аналогичную лингвистическую шкалу, как и для вредоносных программ:

1. Низкая опасность (эффективность) [0 – 3.99].
2. Средняя опасность (эффективность) [4.0 – 6.99].
3. Высокая опасность (эффективность) [7.0 – 8.99].
4. Критическая опасность (эффективность) [9.0 – 10.0].

Таким образом, для вредоносных программ с низкой опасностью будут применены организационные меры с низкой эффективность и т.д.

**Опрос высококвалифицированных специалистов**

Для формирования обучающей и тестовой выборки определены 15 мер обеспечения информационной безопасности и цели, достигаемые при их реализации. Далее, проведен опрос среди 10 высококвалифицированных специалистов в области обеспечения информационной безопасности автоматизированных систем специального назначения. В результате опроса получены оценки эффективности организационных мер, представленные в таблице 1.

*Таблица 1*

*Результаты опроса*

| № п/п | Достигнутые цели | Эффективность реализации меры |
|---|---|---|
| 1 | $m_1$, $m_2$, $m_3$, $m_4$, $m_5$ | 9,78 |
| 2 | $m_1$, $m_3$, $m_5$ | 5,92 |
| 3 | $m_1$, $m_4$ | 6,15 |
| 4 | $m_3$, $m_5$ | 3,07 |
| 5 | $m_4$, $m_5$ | 3,3 |
| 6 | $m_2$, $m_4$, $m_5$ | 5,42 |
| 7 | $m_1$, $m_2$ | 7,09 |
| 8 | $m_3$, $m_4$ | 3,68 |
| 9 | $m_1$, $m_5$ | 5,54 |
| 10 | $m_2$, $m_5$ | 4,25 |
| 11 | $m_2$, $m_3$ | 4,63 |
| 12 | $m_1$, $m_3$, $m_4$ | 7,09 |
| 13 | $m_1$, $m_2$, $m_3$ | 8,04 |
| 14 | $m_3$, $m_4$, $m_5$ | 4,25 |
| 15 | $m_1$, $m_3$, $m_4$, $m_5$ | 8,1 |

**Формирование модели для оценки эффективности организационных мер**

Формирование модели для оценки эффективности организационных мер выполним в комплексе прикладных программ Excel и STATISTICA. В нашем случае целесообразно использовать множественную линейную регрессию [8]. Для этого внесем результаты опроса, в столбце с достигаемыми целями выставляя значение «1», а с недостигаемыми «0».

Результат внесения представлен на рис. 1.

| | E | m1 | m2 | m3 | m4 | m5 |
|---|---|---|---|---|---|---|
| 1 | 10 | 1 | 1 | 1 | 1 | 1 |
| 2 | 6,6 | 1 | 0 | 1 | 0 | 1 |
| 3 | 5,75 | 1 | 0 | 0 | 1 | 0 |
| 4 | 2,5 | 0 | 0 | 1 | 0 | 1 |
| 5 | 3,1 | 0 | 0 | 0 | 1 | 1 |
| 6 | 6 | 0 | 1 | 0 | 1 | 1 |
| 7 | 7,5 | 1 | 1 | 0 | 0 | 0 |
| 8 | 3 | 0 | 0 | 1 | 1 | 0 |
| 9 | 5,7 | 1 | 0 | 0 | 0 | 1 |
| 10 | 3,25 | 0 | 1 | 0 | 0 | 1 |

*Рис. 1. Сведения об опросе в пакете прикладных программ*

В результате моделирования получим следующую модель:

$$E = 0{,}72 + 3{,}9 \times m_1 + 2{,}17 \times m_2 + 1{,}03 \times m_3 + 1{,}45 \times m_4 + 0{,}88 \times m_5,$$

где:

E –значение эффективности реализованной организационной меры,

$m_{1..5}$ – достигаемые цели реализации меры.

Достоверность модели подтверждается сведениями, представленными в рис. 2.

| *Регрессионная статистика* | |
|---|---|
| Множественный R | 0,987258 |
| R-квадрат | 0,974678 |
| Нормированный R-квадрат | 0,943026 |
| Стандартная ошибка | 0,571693 |
| Наблюдения | 10 |

*Рис. 2. Оценка адекватности сформированной модели*

**Верификация модели для оценки эффективности организационных мер**

Верификация сформированной модели будет заключаться в сравнении результатов опроса экспертов и значений, полученных с использованием модели. Результаты верификации представлены в таблице 2.

*Таблица 2*

*Верификация модели*

| № п/п | Достигнутые цели | Эффективность реализации меры (опрос) | Эффективность реализации меры (модель) |
|---|---|---|---|
| 1. | $m_2$, $m_3$ | 4,63 | 4,03 |
| 2. | $m_1$, $m_3$, $m_4$ | 7,09 | 7,1 |
| 3. | $m_1$, $m_2$, $m_3$ | 8,04 | 7,92 |
| 4. | $m_3$, $m_4$, $m_5$ | 4,25 | 4,08 |
| 5. | $m_1$, $m_3$, $m_4$, $m_5$ | 8,1 | 7,98 |

Результаты верификации подтверждают точность модели и непротиворечивость результатов моделирования.

## Заключение

Таким образом, в ходе формирования модели для оценки эффективности организационных мер обеспечения информационной безопасности решены следующие задачи:

1. Определен перечень целей реализации организационных мер обеспечения информационной безопасности (5 целей).

2. Проведен опрос среди высококвалифицированных специалистов, по эффективности реализуемых мер (15 мер).

3. С использованием пакета прикладных программ сформирована модель для оценки эффективности организационных мер обеспечения информационной безопасности.

4. Выполнена ее верификация на тестовом наборе данных.

Результаты данной работы могут быть использованы должностными лицами, ответственными за обеспечение информационной безопасности автоматизированных систем специального назначения для определения перечня необходимых мер при появлении неизвестной вредоносной программы.

## Список литературы

1. Методический документ Методика оценки угроз безопасности информации Утвержден ФСТЭК России 5 февраля 2021 г.

2. Мельников А.В. Подход к оценке опасности деструктивных воздействий вредоносных программ на автоматизированные системы специального назначения / А.В. Мельников, Н.С. Кобяков // Безопасность информационных технологий. – 2023. – Т. 30, № 3. – С. 51-60. – DOI 10.26583/bit.2023.3.03. – EDN RJWWZH.

3. Кобяков Н.С. Оценка опасности вредоносных программ классов «Троянские программы» / Н.С. Кобяков // Альманах Пермского военного института войск национальной гвардии. – 2023. – № 2(10). – С. 31-38. – EDN OYZHVV.

4. Мельников А.В. Модель оценки опасности вредоносных утилит / А.В. Мельников, В.И. Сумин, Н.С. Кобяков // Промышленные АСУ и контроллеры. – 2023. – № 7. – С. 33–40. – DOI 10.25791/asu.7.2023.1448. – EDN KBALDV.

5. Мельников А.В. Модели и алгоритмы реализации организационных мер защиты информации в АССН от деструктивных воздействий ранее неизвестных вредоносных программ / А.В. Мельников, Н.С. Кобяков, Р.А. Жилин // Вестник Воронежского института МВД России. – 2023. – № 3. – С. 80-87. – EDN ZILKNA.

6. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. – Воронеж: Кварта, 2018. – 588 с. ISBN 978-5-93737-158-4.

7. Сумин В.И. Разработка логико-математических моделей принятия управленческих решений в сложных организационных системах специального назначения / В.И. Сумин, А.В. Мельников, В.И. Анциферова, С.А. Сазонова // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 26-34. – DOI 10.12737/2219-0767-2023-16-1-26-34. – EDN NGLTFU.

8. Данилова О.Ю. Правовая статистика: методы и модели / О.Ю. Данилова, В.В. Меньших, С.В. Синегубов. – Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2018. – 302 с. – ISBN 978-5-88591-666-0. – EDN YOZXWX.

## DEVELOPMENT OF A MODEL FOR ASSESSING THE EFFECTIVENESS OF ORGANIZATIONAL MEASURES TO ENSURE INFORMATION SECURITY OF ASSN USING REGRESSION ANALYSIS

***N.S. Kobyakov***

Perm Military Institute of National Guard Forces of the Russian Federation

**Annotation.** The article discusses issues of assessing the effectiveness of organizational measures to ensure information security aimed at training users of automated special-purpose systems. Regression analysis is used to form the model. The results of the work can be used by officials responsible for ensuring information security to prepare users for the operation of automated systems in the context of the implementation of the destructive functions of unknown malicious programs.
**Keywords:** *information security, automated system, malware.*

## ВЛИЯНИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ НА ПСИХОЛОГИЧЕСКОЕ СОСТОЯНИЕ ЧЕЛОВЕКА И ЕГО ПОВЕДЕНИЕ В ОБЩЕСТВЕ

***Д.С. Маликов, А.С. Мелихов***

Пермский военный институт войск национальной гвардии
Российской Федерации

**Аннотация:** В данной работе рассматривается влияние информационной войны на психологическое состояние человека и его поведение в обществе. Анализируются методы и техники, используемые в информационных войнах. Обсуждаются психологические механизмы, которые делают людей уязвимыми перед информационными атаками, а также их последствия для социального взаимодействия. Предлагаются рекомендации по снижению негативного воздействия информационных войн на человека.
**Ключевые слова:** *информационная война, психологическое состояние, поведение в обществе, информационные атаки, уязвимость, социальное взаимодействие, воздействие на человека*.

В эпоху цифровых технологий и мгновенного обмена информацией, понятие когнитивной войны становится все более актуальным. Однако за кулисами хакерских атак и массового распространения заведомо ложных новостей, скрывается нечто более глубокое – воздействие на психику человека и его поведение в обществе. По словам Наталии Красовской (рис. 1), политического психолога, кандидата психологических наук, информационная война – «борьба за умы людей, наносящая обществу тяжёлую культурно-психологическую травму, от которой очень сложно оправиться» [3]. Информация проникает в повседневную жизнь людей, сказываясь на их психологическом состоянии и поведенческих реакциях. Она способствует усилению поляризации общества, разделяя людей на группы с противоположными взглядами и усиливая конфликты. Чрезмерное воздействие манипулятивных техник приводит к изменению восприятия реальности и формированию мнений, подкрепленных ложными фактами. Постоянный поток негативной информации может снизить мотивацию людей к участию в общественной жизни из-за ощущения бесполезности и безысходности. Множество источников, часто представляющих противоречивые сообщения, создают путаницу, вносят неопределенность и стресс в сознание индивида. Этот феномен, оказывая давление на человека и его поведение в обществе, становится предметом все более широкого изучения и вызывает растущий интерес среди исследователей, практиков и общественности в целом.


*Рис. 1. Наталия Красовская – политический психолог, кандидат психологических наук*

Когнитивная война представляет собой стратегический подход, в рамках которого информационные ресурсы используются для воздействия на мышление человека, изменение его ценностей и поляризацию необходимого мнения в обществе с целью достижения определенных политических, экономических или

военных целей. В отличие от традиционных форм конфликтов, информационная война оперирует не столько физической силой, сколько влиянием на противника, манипуляцией фактами и формированием определенных представлений. Основные способы включают в себя использование различных медиаплатформ, социальных сетей, новостных и интернет-источников для распространения специально подобранной информации, которая может быть как правдивой, так и ложной, но ее основная задача – воздействовать на восприятие и убеждения аудитории. Этот вид конфликта, обладающий множеством тонких методов и стратегий, часто бывает невидимым и не ограничивается территориальными границами, что делает его особенно сложным для обнаружения и противодействия.

Опасность информационной войны не ограничивается лишь поверхностным воздействием, ее последствия проникают глубже. Массовые манипуляции, вызванные фальсификациями и приводящие к формированию определенных стереотипов или предубеждений, могут создать атмосферу неопределенности, страха и подрыва доверия к новостным источникам. Кроме того, кибератаки, характерные для данных войн, представляют серьезную угрозу для стабильности и безопасности, ведь возможность осуществления атак на системы государства и предприятий могут привести к дестабилизации экономики и общества в целом. Таким образом, война выходит за пределы простого воздействия на информационные потоки, что требует разработки эффективных методов противостояния.


*Рис. 2. Джордж Буш-старший и Арнольд Шварценеггер во время предвыборной кампании в 1992 году*

В наше время, когда информация представляет собой огромный поток данных, все сложнее отфильтровать её для обработки. Выделить необходимую информацию становится труднее из-за насыщенности лозунгами, агитацией и пропагандой. Очевидно, что влиять на людей легко, если знать, как это делать правильно. Наше сознание постоянно подвергается попыткам манипуляции через различные методы и техники. Чтобы противостоять им, необходимо уметь распознавать различные виды и способы пропаганды. Один из ключевых подходов заключается в использовании авторитетных личностей или групп влияния для привлечения внимания целевой аудитории. Эти авторитеты могут включать в себя известных политических деятелей, руководителей предприятий, преподавателей высших и средних учебных заведений, деятелей культуры, известных актеров. Эффективность этого метода зависит от уровня доверия, который представитель группы влияния имеет у целевой аудитории, а также от степени его известности. Так, в ходе избирательных кампаний часто привлекают известных артистов, которые активно поддерживают того или иного кандидата. В ряде случаев они даже вступают в состав определенных политических движений, что способствует улучшению репутации этих движений. Например, в 1992 году известный киноактер Арнольд Шварцнеггер выступил в поддержку Джорджа Буша на выборах Президента США (рис. 2).

Помимо основного подхода, существуют и другие теории информационных войн, представляющие разнообразные стратегии и тактики. Одной из таких теорий является «Имитационная дезинформация». Этот подход включает в себя изменение пропаганды противоположной стороны с целью снижения доверия к ней и формирования негативного образа. Другой теорией является «Псевдологические выводы», которая основана на использовании ложных выводов, которые преподносятся как логически верные, для воздействия на мнение целевой аудитории. Также существует «Принуждающая пропаганда», воздействующая на общественное мнение через использование слов и выражений с принуждающим характером. К таковым можно отнести расклеивание листовок или распространение сообщений с агитацией к какому-либо действию. Наибольшую популярность в наши дни набирает способ воздействия на общество с помощью «Массовых вбросов». Они характеризуются резким заполнением всевозможных источников информацией, которая носит яркий эмоциональный окрас и нередко является профессионально переработанной правдой в негативном ключе. Таким образом, видя подобную новость и слепо доверяя ей, основываясь на том, что о ней говорят массово, люди становятся более уязвимыми и легче поддаются на дальнейшие уловки, поэтому при восприятии известий, которые внезапно появляются на множестве ресурсов и вызывают широкий спектр эмоциональных реакций от сочувствия до негодования, важно осознавать возможность попадания под воздействие информационного вброса. Присутствие хорошо

структурированной текстовой составляющей и эмоциональная насыщенность часто являются признаками данного явления.

В связи с последними событиями, касающимся всего мира в целом, психологи считают: «Субъективно можно сказать, судя по поведению людей в социальных сетях, цифровых платформах и мессенджерах, – многие в моральной панике». Социальные сети полны «свидетельств с мест», когда показывают настоящие и ненастоящие фото и видео с подачей нужной интерпретации, что является инструментом информационной войны и ведет к появлению хаоса и морального дисбаланса.

Чтобы сделать общество более устойчивым к информационным атакам, необходимо принимать комплекс мер, охватывающих различные аспекты образования, информационной грамотности, технических защит и сознательной критической мысли. Важным шагом является повышение информационной грамотности, которое включает в себя не только умение различать достоверные и ложные источники информации, но и анализ контента, осознание мотивов за информационными кампаниями и развитие способности к самокритике. Образовательные программы, медиаобразование и обучение критическому мышлению играют ключевую роль в формировании у общества этих навыков. Но тем не менее не стоит забывать о важности современных средств киберзащиты от хакерских атак, укреплении сетевой безопасности и разработки механизмов фильтрации информации для идентификации и блокировки нежелательных искаженных сообщений. Помимо этого, важно поощрять активное участие граждан в общественной жизни и укреплять доверие к независимым источникам информации. Создание и поддержка платформ для обсуждения и диалога, где каждый может высказать свою точку зрения, а также поощрение медиа, следующих высоким журналистским стандартам, способствуют формированию здоровой информационной среды.

*Рис. 3. Михаил Вершинин, социальный психолог*

Однако, абсолютной защиты от информационной войны не существует. «Вы не избежите информационного влияния, так как мы постоянно потребляем новости и различный политический контент», – говорит социальный психолог, Михаил Вершинин (рис. 3) [2]. Вместо этого необходимо стремиться к созданию устойчивого общества, осознающего свои слабые места и способное реагировать на вызовы информационных атак. Реализация этих мер поможет создать более устойчивое и информированное общество, способное противостоять информационным угрозам в современном мире.

## Список литературы


1. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. 124 с. URL: https://mgimo.ru/upload/iblock/486/%D0%A1%D1%83%D0%BB%D0%B5%D0%B9%D0%BC%D0%B0%D0%BD%D0%BE%D0%B2%D0%B0%20%D0%A8.%D0%A1.%20%D0%9D%D0%B0%D0%B7%D0%B0%D1%80%D0%BE%D0%B2%D0%B0%20%D0%95.%D0%90.%20-%20%D0%98%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%98%D0%9E%D0%9D%D0%9D%D0%AB%D0%95%20%D0%92%D0%9E%D0%99%D0%9D%D0%AB.pdf

2. Социальный психолог Михаил Вершинин о том, как не стать жертвой информационной войны – Рамблер/финансы (rambler.ru) URL: https://finance.rambler.ru/money/48236315-sotsialnyy-psiholog-mihail-vershinin-o-tom-kak-ne-stat-zhertvoy-informatsionnoy-voyny/?ysclid=lp5xsfa15z362935336

3. «Им нужен ваш мозг»: как влияют на человечество информационные войны | ПОЛИТИКА | АиФ Новосибирск (aif.ru) URL: https://nsk.aif.ru/politic/im_nuzhen_vash_mozg_kak_vliyayut_na_chelovechestvo_informacionnye_voyny?ysclid=lp5xpshpno772970789

4. Федорова О.Н. Информационно-психологическая безопасность личности в информационном обществе / О.Н. Федорова // Вестник Дальневосточного государственного технического университета. – 2011. – № 2(7). – С. 21–34. – EDN SZGXNT. URL: https://www.elibrary.ru/download/elibrary_22541053_37046639.pdf

5. Джура Г.С. Информационно-психологическая безопасность личности в современных реалиях / Г.С. Джура // Вестник Донецкого национального университета. Серия Д: Филология и психология. – 2022. – № 3. – С. 119–122. – EDN TZUVUY. URL: https://www.elibrary.ru/download/elibrary_53876141_58059365.pdf

6. Ряжапов Н.Х. Национальные интересы России в информационной сфере в условиях мировой нестабильности и меры их обеспечения / Н. Х. Ряжапов // Развитие науки и образования в условиях мировой нестабильности: современные парадигмы, проблемы, пути решения : Материалы Международной

научно-практической конференции. В 2-х частях, Ростов-на-Дону, 29 октября 2021 года. Том Часть 1. – Ростов-на-Дону: ООО «Издательство ВВМ», 2021. – С. 101–110. – EDN ESSRPG. URL: https://www.elibrary.ru/download/elibrary_47231698_67351052.pdf

7. Морозов А.В. Психология информационной провокации / А.В. Морозов // Казанский педагогический журнал. – 2017. – № 6(125). – С. 27–35. – EDN ZTWRGP. URL: https://www.elibrary.ru/download/elibrary_30611528_51412637.pdf

8. Манойло, А. В. Информационные войны / А. В. Манойло // Геополитический журнал. – 2017. – № 5–6(20). – С. 28-36. – EDN YVAZFA. URL: https://www.elibrary.ru/download/elibrary_32751839_91412484.pdf

## THE IMPACT OF INFORMATION WARFARE ON THE PSYCHOLOGICAL STATE OF A PERSON AND HIS BEHAVIOR IN SOCIETY

***D.S. Malikov, A.S. Melikhov***

Perm Military Institute of National Guard Forces of the Russian Federation

**Annotation.** This paper examines the impact of information warfare on the psychological state of a person and his behavior in society. The methods and techniques used in information wars are analyzed. The psychological mechanisms that make people vulnerable to information attacks, as well as their consequences for social interaction, are discussed. Recommendations are offered to reduce the negative impact of information wars on humans.

**Keywords:** *Information war, psychological state, behavior in society, information attacks, vulnerability, social interaction, human impact.*

## ЦИФРОВАЯ ГРАМОТНОСТЬ НАСЕЛЕНИЯ

***А.С. Мелихов, Ю.В. Некрасов***

Пермский военный институт войск национальной гвардии
Российской Федерации

**Аннотация.** В статье рассмотрены вопросы, относящиеся к понятию «цифровой грамотности» населения, показана важность владения населением компетенциями, относящимися к области цифровой грамотности. Выявлены способы увеличения уровня цифровой грамотности населения. Рассмотрены результаты проведения всероссийской акции «Цифровой диктант», проанализирован средний уровень цифровой грамотности населения страны, а также индекс цифровой грамотности НАФИ.

**Ключевые слова:** *цифровая грамотность, уровень цифровой грамотности населения, цифровое образование, цифровой диктант, цифровизация*.

Развитие цифровых технологий, функционирование в рамках цифровой среды требуют наличия определенных знаний и навыков, получивших название «цифровой грамотности», или «цифровой компетентности». Формирование данных умений у населения происходит как в ходе обучения в системе образования, так и в ходе накопления непосредственного опыта взаимодействия с цифровой средой. В результате различий в условиях и длительности формирования цифровых компетенций и навыков уровень цифровой грамотности разных групп населения различается, формируется неоднородность населения по данному признаку, что особенно проявляется в сравнении разных возрастных категорий.

Цифровая грамотность населения – это способность людей использовать цифровые технологии, устройства и интернет для достижения своих целей и решения задач в различных сферах жизни. Она включает в себя знания, навыки и умения, необходимые для безопасного и эффективного использования цифровых ресурсов, а также умение критически оценивать и анализировать информацию, полученную из цифровых источников [1, С. 33].

Повышение цифровой грамотности населения способствует развитию информационной культуры общества, улучшению качества жизни людей и обеспечению их доступа к информации и знаниям. Это также помогает снизить цифровой разрыв между различными группами населения и способствует развитию цифровой экономики.

Цифровая грамотность включает в себя умение пользоваться поисковыми системами и находить нужную и полезную информацию, способность отличить добросовестные и вызывающие доверие источники информации от недобросовестных, знание о системах родительского контроля и умение ими пользоваться. Также пользователи должны понимать, что в интернете не стоит выкладывать лишнюю информацию о себе и своих персональных данных, чтобы не стать жертвой мошенников и злоумышленников [2, С. 154].

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации ведет работу по оценке текущего состояния и перспектив изменения уровня цифровой грамотности населения Российской Федерации.

Так, например, с аналитический центр Национальное агентство финансовых исследований (НАФИ) представляет результаты ежегодной комплексной оценки текущего уровня сформированности компетенций цифровой экономики у населения России и готовности россиян к жизни в условиях цифровизации. Исследования проводятся с использованием платформы для оценки цифровой грамотности «Цифровой гражданин» [3].

Индекс цифровой грамотности измеряется в процентных пунктах (п.п), его значение может варьироваться от 0 до 100. Индекс отражает компетенции

россиян в сфере информационной грамотности, коммуникативной грамотности, создания цифрового контента, цифровой безопасности и решения проблем в цифровой сфере [3].

По результатам оценки за 2022 год индекс цифровой грамотности россиян составил 71 п.п (табл. 1).

*Таблица 1*

*Динамика Индекса цифрой грамотности НАФИ в период в 2018 по 2022 годы*

| | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| Индекс цифровой грамотности НАФИ (в процентных пунктах) | 52% | 52% | 58% | 64% | 71% |

С начала измерений в 2018 году индекс цифровой грамотности россиян демонстрирует уверенный рост с 52 до 71 п.п.

Две трети россиян (69%) на сегодняшний день обладают базовым уровнем цифровой грамотности. Менее трети (29%) – продвинутым. 2% жителей России имеют начальный уровень цифровой грамотности (Таблица 2).

*Таблица 2*

*Доля населения, обладающего разными уровнями цифровой грамотности 2020–2022 гг.*

| | 2020 | 2021 | 2022 |
|---|---|---|---|
| Начальный уровень, п.п. | 7 | 3 | 2 |
| Базовый уровень, п.п. | 66 | 70 | 69 |
| Продвинутый уровень, п.п. | 27 | 27 | 29 |

В динамике за два года доля населения с начальным уровнем цифровой грамотности падает, с продвинутым и базовым растет. Так, рост доли тех, кто демонстрирует уверенные знания и компетенции в цифровой среде, с 2020 года выросла на 2 п.п. (с 27% до 29%), средние – 3 п.п. (с 66% до 69%). Доля россиян, плохо разбирающихся в цифровых технологиях, сократилась на 5 п.п. (с 7% до 2%).

Также следует отметить, что Минцифры России рассчитывают к 2024 году довести уровень цифровой грамотности жителей страны до 75%, одним из проектов по достижению данной цели станет новый сезон просветительского проекта в сфере цифровой грамотности и кибербезопасности «Цифровой ликбез», проводимый VK и АНО «Цифровая экономика» [4].

Проект «Цифровой ликбез» основан на создании образовательных видеороликов, с помощью которых будет обучение школьников азам цифровой грамотности и правилам кибербезопасности в современном мире. В роликах

расскажут, как распознать фишинговую ссылку, защитить личную информацию в сети или как правильно действовать, столкнувшись с кибербуллингом [4].

Одним из методов оценивания цифровой грамотности населения является проведение всероссийской акции «Цифровой диктант». Это самая масштабная акция по проверке знаний в сфере интернет-технологий. Пользователи смогут узнать свой индивидуальный уровень цифровых компетенций как в онлайн-, так и в офлайн-формате.

Цифровой Диктант – Всероссийская акция, признанная самой масштабной в России проверкой знаний в области цифровой грамотности. Акция дает возможность пользователям не только узнать свой уровень цифровых компетенций, но и пройти работу над ошибками, а также сформировать свою личную стратегию развития недостающих знаний и навыков [6].

Диктант состоит из тестирований, разработанных с учетом разных возрастных категорий:

– для детей (10–13 лет);

– подростков (14–17 лет);

– взрослых (18–59 лет);

– люди старшего возраста (60 лет и старше) [6].

Каждое тестирование включает 4 смысловых блока.

Первый блок посвящен основам цифрового потребления, а именно, различным устройствам и знаниям базовых программ и приложений.

Второй – цифровым компетенциям (работе с интернетом, социальными сетями, интернет-магазинами и другими онлайн-сервисами).

Третий – цифровой безопасности, в том числе защите своих персональных данных и устройств. Четвертый дополнительный блок – новым технологиям, включая искусственный интеллект и умные голосовые помощники.

Цифровой Диктант также позволяет познакомиться с цифровыми сервисами и продуктами, в том числе отечественного производства.

Диктант проводится с 2019 года и каждый год набирает все большую популярность. Так, например, на рисунке 1 видно, что количество участников диктанта увеличилось более чем в 35 раз с 39 398 человек до 1 385 643 человек.

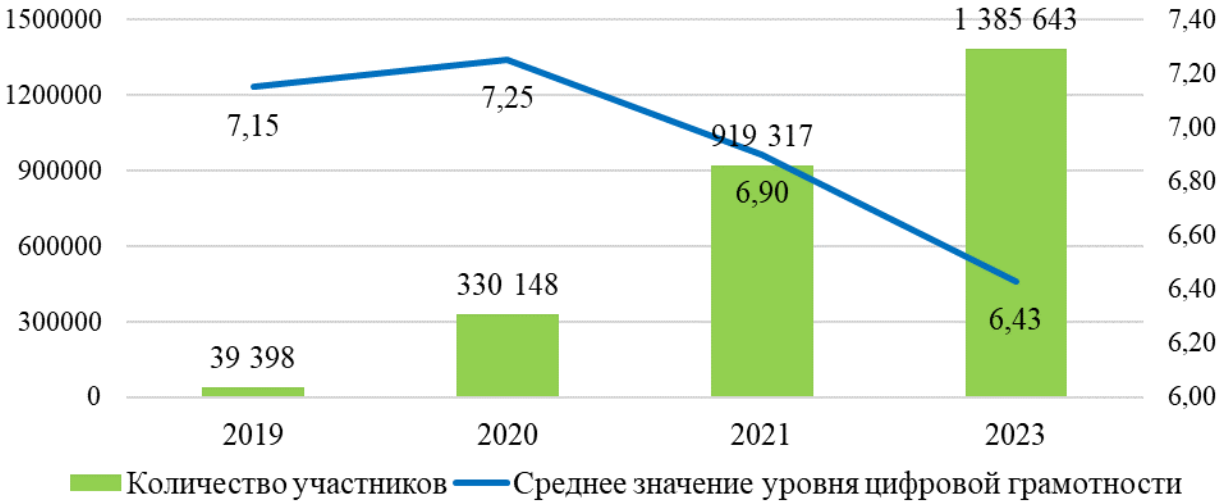



*Рис. 1. Динамика результатов участников в 2019–2023 гг.*

Также следует отметить, что среднее значения уровня цифровой грамотности участников диктанта снизился на 0,72 балла с 7,15 баллов до 6,43 баллов.

По итогам цифрового диктанта 2023 года наиболее высокие значения показали аудитории 26–35 и 36–45 лет – 6,96 балла и 6,73 балла соответственно. Наименьший показатель наблюдается среди крайних возрастных групп – старше 60 лет (6,19 балла) и меньше 10 лет (6,06 балла) (рис. 2).

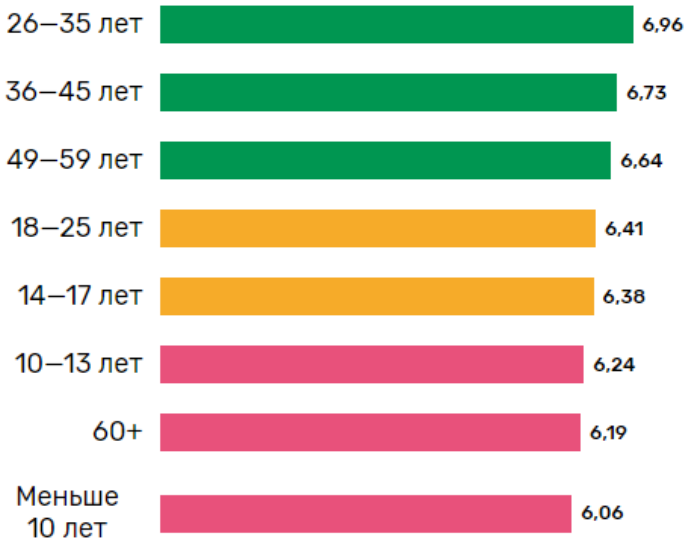



*Рис. 2. Среднее значение уровня цифровой грамотности участников акции Цифровой диктант по возрастным категориям в 2023 г. (по 10-бальной шкале)*

По регионам наилучшей цифровой грамотностью по всем четырём блокам диктанта обладают участники из Москвы, Астраханской и Архангельской области, а также из Республики Карелия (табл. 3) [6].

*Таблица 3*

*Рейтинг регионов по результатам проведения Цифрового диктанта в 2023 году*

| Место | Цифровая грамотность | Цифровое потребление | Цифровые компетенции | Цифровая безопасность |
|---|---|---|---|---|
| 1 | г. Москва Республика Карелия (7,34) | Архангельская область (7,31) | г. Москва (7,28) | Республика Карелия (7,74) |
| 2 | Астраханская область (7,26) | г. Москва (7,23) | Астраханская область (7,25) | г. Москва (7,53) |
| 3 | Архангельская область (7,06) | Астраханская область (7,22) | Республика Карелия (7,08) | Чувашская республика – Чувашия (7,36) |
| 85 | Республика Тыва (5,28) | Республика Ингушетия (5,42) | Республика Ингушетия (5,09) | Республика Дагестан (5,9) |
| 86 | Чеченская Республика (5,01) | Чеченская Республика (5,03) | Республика Тыва (4,77) | Республика Ингушетия (5,54) |
| 87 | | Республика Тыва (5,02) | Чеченская Республика (4,68) | Чеченская Республика (5,33) |

Наихудшие показатели цифровой грамотности населения наблюдаются в Чеченской республики, в Республике Тыва, Ингушетия и Дагестан.

Цифровая грамотность является важным навыком для современного человека, так как она позволяет людям эффективно использовать цифровые технологии и ресурсы для достижения своих целей. Она также помогает защитить пользователей от возможных угроз и проблем, связанных с использованием цифровых технологий. Цифровая грамотность способствует развитию инноваций и созданию новых возможностей в различных отраслях, таких как образование, здравоохранение, экономика, поэтому очень важно улучшать уровень цифровой грамотности среди всех слоев и возрастов населения [5].

Для развития уровня цифровой грамотности населения следует необходимо:

1. Проводить образовательные программы и мероприятий, направленные на обучение людей использованию цифровых технологий и ресурсов;

2. Создавать доступные и удобные цифровые сервисы и услуги для различных групп населения;

3. Разрабатывать и внедрять стандарты и норм, обеспечивающие безопасность и качество цифровых продуктов и услуг;

4. Поддерживать инициативы, направленные на развитие цифровой грамотности, таких как проведение цифровых диктантов и конкурсов как на местном уровне, так и на всероссийских.

5. Развивать инфраструктуру и обеспечение доступа к интернету для всех слоев населения;

6. Продвигать идей цифровой грамотности среди молодежи и образовательных учреждений;

7. Привлекать внимание общественности к вопросам цифровой грамотности и информационной безопасности.

Среди направлений цифровой грамотности населения можно выделить:

– Обучение людей использованию цифровых технологий для решения повседневных задач;

– Повышение безопасности и конфиденциальности в интернете;

– Развитие навыков работы с большими данными и искусственным интеллектом;

– Обучение навыкам работы с новыми технологиями, такими как блокчейн, криптовалюты и интернет вещей;

– Поддержка инициатив, направленных на создание доступных и удобных цифровых сервисов для различных групп населения.

Таким образом, как и «обычная» грамотность, цифровая грамотность является важным фактором достижения жизненных целей, повышения качества и уровня жизни населения.

В ближайшем будущем надлежащее измерение цифровой грамотности и корректировка принимаемых мер поддержки и программ должны привести к повышению производительности, укреплению конкурентоспособности как отдельных граждан, так и бизнеса, и в конечном итоге – к росту национальных экономик.

## Список литературы

1. Гарифуллина А.Фа., Мурзина Э.Ф., Хужин Р.А. ЦИФРОВАЯ ГРАМОТНОСТЬ НАСЕЛЕНИЯ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ // Гуманитарные, социально-экономические и общественные науки. 2022. №11–1. С. 33–35 [Электронный ресурс] URL: https://cyberleninka.ru/article/n/tsifrovaya-gramotnost-naseleniya-problemy-i-puti-resheniya

2. Ельцова О.В., Емельянова М.В. К вопросу о понятии цифровой грамотности // Вестник ЧГПУ им. И.Я. Яковлева. 2020. № 1 (106). С. 155–161 [Электронный ресурс] URL: https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-tsifrovoy-gramotnosti

3. В России выросла доля людей с продвинутым уровнем цифровой грамотности от 30.03.2023 // Национальное агентство финансовых исследований URL: [Электронный ресурс] https://nafi.ru/analytics/v-rossii-vyrosla-dolya-lyudey-s-prodvinutym-urovnem-tsifrovoy -gramotnosti/

4. Уровень цифровой грамотности россиян планируют повысить до 75 процентов от 10.01.2023 // РИА Новости [Электронный ресурс] URL: https://ria.ru/20230110/ tsifrovizatsiya-1843855662.html

5. Официальный сайт Министерства цифрового развития, связи, и массовых коммуникаций Российской Федерации [Электронный ресурс] URL: https://digital.gov.ru/ ru/activity/ directions/540/?utmreferrer=https%3a%2f%2 fyandex.ru%2f

6. Официальный сайт проекта «Цифровой диктант» [Электронный ресурс] URL: https://digitaldictation.ru/

## DIGITAL LITERACY OF THE POPULATION

***A.S. Melikhov, Yu.V. Nekrasov***
Perm Military Institute of National Guard Forces of the Russian Federation

**Abstract.** The article discusses issues related to the concept of «digital literacy» of the population, shows the importance of the population's possession of competencies related to the field of digital literacy. The ways of increasing the level of digital literacy of the population have been identified. The results of the All-Russian campaign «Digital Dictation» are considered, the average level of digital literacy of the country's population is analyzed, as well as the NAFI digital literacy index.
**Keywords***: digital literacy, the level of digital literacy of the population, digital education, digital dictation, digitalization.*

## АНАЛИЗ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СВЯЗИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ТРЕНИРОВОЧНЫХ КАРТ ПО НАСТРОЙКЕ И ПРИМЕНЕНИЮ РАДИОСТАНЦИЙ В РЕЖИМЕ ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКИ РАБОЧИХ ЧАСТОТ

***А.С. Мелихов, Д.А. Морев***
Пермский военный институт войск национальной гвардии Российской Федерации

**Аннотация.** В данной статье рассматривается актуальность применения режима псевдослучайной перестройки рабочих частот в средствах связи, и проанализированы действия войск во время проведения специальной военной операции при действиях на средства связи средств радиоэлектронной борьбы.
**Ключевые слова:** *подготовка специалистов, помехоустойчивость средств радиосвязи, борьба с организованными помехами средств связи***.**

В современной теории военного противоборства все большее значение придается внедрению новых систем управления, основанных на сетецентрических принципах, при этом основой такой системы управления является подси-

стема связи. В этой связи с одной стороны системы связи должны соответствовать жестким требованиям системы управления войсками и оружием, с другой стороны в условиях современного противоборства они сами подвергаются деструктивному воздействию со стороны противника. Основой современного деструктивного воздействия на системы радиосвязи является применение средств радиоэлектронной борьбы и радиоэлектронного подавления. Целью статьи являются анализ соответствия возможностей режима работы псевдослучайная перестройка рабочей частоты и обоснование разработки учебно-тренировочной карты и программы для электронно-вычислительных машин для дальнейшего повышения эффективности обучения специалистов связи.

Технология ППРЧ это вид передаваемой информации по радиоканалам, главной особенностью которого является передача информации частот. Так отправителю, так и получателю известна частота, по которой будет передаваться информация согласно «Псевдослучайной последовательности чисел». Псевдослучайная перестройка рабочей частоты-метод передачи информации по радио, особенность которого заключается в частой смене несущей частоты. Метод повышает помехозащищённость канала связи и не только.

В целях построения сигналов будет использоваться частотно-временные матрицы, в которой каждые столбцы являются временными позициями, а строчки согласно условному номеру частоты.

Метод псевдослучайной перестройки рабочей частоты используется как в военной, так и в гражданской сфере. При использовании данного метода, сигнал становится устойчивым к глушению, что даёт его использовать в военной сфере деятельности.

Известно, что важнейшими составляющими помехозащищённости средств радиосвязи, является помехоустойчивость и скрытность.

Под помехоустойчивостью средств радиосвязи с ППРЧ понимается способность нормального функционирования и выполнения задач по приёму и передаче информации в условиях действия радиопомех.

Следовательно, помехоустойчивость средств радиосвязи – это способность противостоять вредному воздействию различного вида радиопомех, включая, в первую очередь, организованные помехи.

Борьба с организованными помехами средств связи с ППРЧ заключается, в «уходе» сигналов от воздействия помех, а не в «противоборстве» с ними. Поэтому в средствах радиосвязи с ППРЧ при защите от помех одной из важнейших характеристик является фактическое время работы на одной частоте. Чем меньше это время, тем выше шанс того, что на сигналы со средств радиосвязи с ППРЧ не будут воздействовать организованные помехи.

Также помехоустойчивость зависит не только от времени работы на одной частоте, но и от других немало важных параметров станции помех и средств радиосвязи, например, от таких как виды помех и их мощности, структура принимающего устройства и заложенных в средства связи способов помехоустойчивости.

Чтобы достигнуть эффективное воздействие помех на средства радиосвязи с ППРЧ может быть достигнуть лишь при условиях знания постановщика помех с соответствующими параметрами сигналов, например, центральную частоту, скорость перестройки частот, ширина полосы частот, мощность сигнала и помехи в точке нахождения приёмного устройства средств радиосвязи. Все эти параметры постановщик помех добывает как правило, при помощи станции радиотехнической разведки, а также пересчёта параметров в средствах связи в другие, связанные с ними, характеристики средств радиосвязи. Так как при измерении длительности скачка частоты, можно определить ширину полосы частотного канала приёмного средства радиосвязи.

Адаптивная автоматизированная связь позволяет радиосредствам автоматизировано анализировать помеховую обстановку на выделенных для работы частотах и переходят в случае необходимости на частоты с минимальным уровнем помех. Техническое маскирование (ТМ) применяется для исключения несанкционированного прослушивания переговоров. Данный режим реализован во всех радиостанциях комплекса Р-168Е. Число ключей, равное 2.128, и алгоритм работы датчика псевдослучайных чисел гарантируют надежное закрытие тактической информации.

После того, как в районе проведения специальной операции на территории Украине массово начали применять и строить системы радиосвязи преимущественно с использованием режимов работы ППРЧ возникла необходимость быстрому и эффективному обучению специалистов связи порядку настройки радиостанций, а готовых понятных и качественных УТК, и другого методического материала для проведения занятий нет, так как этому вопросу не уделялось должного внимания.

Изучая программу боевой подготовки войск в рамках которой проходит подготовка специалистов радиосвязи, а также тематических планов по дисциплинам в учебных заведениях ВНГ РФ обнаружил факт, что до февраля 2022 года целенаправленно такой режим работы радиостанций, как ППРЧ не изучался и только после поступления распоряжения с центрального аппарата войск начали вносится изменения в учебные планы и планы боевой подготовки.

После того, как были определены тематические планы и время на проведения занятий была выявлена очередная проблема в подразделениях нет достаточно нужных средств(техники) связи для охвата всех обучающихся на занятии, а в случаи наличия средств(техники) связи необученность алгоритму настройки и нарушение порядка подготовки радиостанций к работе приводил к выходу из строя радиостанций. Поэтому мне было поручено разработать УТК «Настройка УКВ радиостанции Р-168-100У-2 в режиме ППРЧ», а также в составе творческого коллектива кафедры связи участвовал в разработке программы для ЭВМ «Программа для обучения специалистов связи порядку настройки радиостанций комплекса «Акведук» в режиме работы ППРЧ» своевременность и важность проведенной работы сложно недооценить. [1]

1. Включить питание радиостанции – тумблер ПИТАНИЕ – ВКЛ.

– Если радиоданные не в введены, на табло высветится «РД Н ЗАП ВВОД?», нажать ВВОД.

– Если радиоданные введены,( на табло показан канал и режим работы) то нажать кнопки «РЖ», «1» ( «Настр.»).

(нажать вкл, ввод)


*Рис. 1. Учебно-тренировочная карта*

Разработанные учебно-методические материалы позволили решить следующие задачи:

– повысить эффективность подготовки радиотелефонистов и специалистов КШМ;

– снизить расход ресурсов средств (техники) связи;

– предотвратить отказ техники связи, связанного с неумелой эксплуатацией на начальном этапе ее освоения;

– обеспечить эффективность проведения следующих видов учебных занятий: групповое занятие, самостоятельная работа под руководством преподавателя, практическое занятие;

– обеспечить проведение планового и внезапного контроля уровня подготовленности по эксплуатации средств связи.

Сами УТК представляют собой последовательность действий обучающегося для достижения нужного результата, в данном случаи это настройка радиостанции в заданном режиме работы с визуализацией рабочей панели радиостанции.

Также была разработана программа для ЭВМ под названием «Программа для обучения специалистов связи порядку настройки радиостанций комплекса «Акведук» в режиме работы ППРЧ» предназначена для обучения специалистов связи воинских частей (организаций) войск национальной гвардии порядку настройки радиостанций комплекса «Акведук» в режиме работы ППРЧ, она обеспечивает: повышение эффективности процесса обучения специалистов связи, формирование у них умений и закрепление навыков эксплуатации радиостанций комплекса «Акведук».[2]


*Рис. 2. Внешний вид программы.*

Программный продукт используется должностными лицами службы связи воинских частей (организаций), профессорско-преподавательским составом военных вузов в учебном процессе при проведении теоретических и практических занятий.

Код программной части реализован средствами среды разработки HTML и JavaScript, для создания дизайна использовались каскадные таблицы стилей(CSS).

Программа позволяет работать в операционной системе как в ОС Microsoft Windows, так и ОС Linux.

Поступившие отзывы из воинских частей Московского гарнизона в виде Актов внедрения научной продукции (приложение Д) свидетельствуют,

что программа для ЭВМ «Программа для обучения специалистов связи порядку настройки радиостанций комплекса «Акведук» в режиме работы ППРЧ» повышает эффективность получения обучающимися навыков и умений при поведении занятий по боевой подготовке.

Для достижения поставленной цели были решены задачи, в ходе которых сделаны следующие выводы и предложения:

Анализ метода радиосвязи с псевдослучайной перестройкой рабочей частоты с точки зрения таких характеристик как помехозащищенности и скрытности показав, что на сегодняшний день эта технология является одной из лучших и использование ее в военной технике связи считается своевременным и актуальным.

Повышение качества обучения в войсках национальной гвардии требует своевременного изменения учебных программ и планов боевой подготовки с точки зрения актуализации относительно выявленных проблем, в том числе полученного опыта в период проведения специальной военной операции на территории Украины с одной стороны и с другой стороны разработка новых учебно-методических материалов в соответствии современным условиям, в том числе и по созданию современной среды обучения. Эти требования заставляют создавать и внедрять в обучение компьютерные анимационные программы.

Разработанные новые учебно-методические материалы позволяют повысить эффективность обучения в войсках национальной гвардии, что подтверждается поступившими отзывами из воинских частей Московского гарнизона в виде Актов внедрения научной продукции.

В дальнейшем исследование данной темы поможет разрабатывать новые способы помехозащищенности систем связи специального назначения.

## Список литературы

1. Макаренко С.И. , Иванов М.С. , Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: монография / С.И. Макаренко, М.С. Иванов, С.А. Попов. – СПб.: Свое издательство, 2013. – С. 159–166.

2. Помехозащищенность радиосистем со сложными сигналами / Г.И. Тузов [и др.] ; под ред. Г.И. Тузова. – М.: Радио и связь, 1985. – С. 261-264.

## ANALYSIS OF THE TRAINING OF COMMUNICATION SPECIALISTS BASED ON THE USE OF TRAINING CARDS FOR SETTING UP AND USING RADIO STATIONS IN PSEUDO-RANDOM MODE ADJUSTMENT OF OPERATING FREQUENCIES

***D.A. Morev, A.S. Melikhov***

Perm Military Institute of National Guard Forces of the Russian Federation

**Abstract.** This article examines the relevance of using the regime of pseudo-random tuning of operating frequencies in communications and analyzes the actions of troops during a special military operation when acting on the communications federation of radio electronic warfare equipment.

**Keywords:** *training of specialists, noise immunity of radio communication means, the fight against organized interference of communication means.*

## ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ ВОЗДЕЙСТВИЮ. ПРОЕКТ «БАРЬЕР»

***А.А. Миклин, М.Д. Дударев, Р.З. Латыпов, А.И. Соскин, В.Ю. Никитина, Е.Ю. Никитина, В.Р. Акишин, Н.Д. Черкасов***

Пермский государственный национальный исследовательский университет

**Аннотация**. В работе рассматривается проблема деструктивного воздействия информации в электронных информационных ресурсах. Актуальность проблемы заключается в широком распространении деструктивной информации и неэффективности существующих способов противодействия деструктивному воздействию. Целью данного исследования является изучение проблемы деструктивного воздействия на личность и разработка метода противодействия. Проведен анализ существующих методов противодействия деструктивному воздействию, в результате которого выявлено, что большинство решений ограничиваются фильтрацией контента или ограничением доступа к определенным сайтам. В данной статье представлен новый способ противодействия деструктивному воздействию. Проект «Барьер» – программа, которая позволяет обнаруживать и скрывать деструктивную информацию на экране монитора, а также предупреждать пользователей о возможных рисках, связанных с такой информацией. Программа является эффективным инструментом для защиты психологического здоровья пользователей от деструктивного воздействия. Результаты тестирования показали, что программа работает стабильно и эффективно обнаруживает, и скрывает деструктивную информацию. Несмотря на рассмотренные проблемные моменты при реализации, программа имеет будущее при дальнейшем ее совершенствовании.

**Ключевые слова**:*Деструктивное воздействие, деструктивная информация, методы противодействия, противодействие деструктивному воздействию, контент-фильтры.*

## Введение

Информационному влиянию в современном мире подвержен каждый. Несмотря на то, что информация окружает нас повсюду, большую её часть современный человек получает из электронных информационных ресурсов, в том числе из сети Интернет. Информация может оказывать на человека различное воздействие, однако наиболее опасным является деструктивное влияние. Все сведения, которые могут нанести или спровоцировать нанесение вреда здоровью человека, являются деструктивной информацией. В первую очередь речь идет о психологическом здоровье, так как деструктивная информация может оказывать воздействие на психику людей, потребляющих данную информацию.

Актуальность проблемы обусловлена тем, что современное российское общество находится в сложном динамическом состоянии из-за масштабных социально-коммуникационных трансформаций. В следствии этого государство сталкивается с новой реальностью, новыми факторами дезорганизации, требующими адекватного реагирования [1]. По данным проекта «Мы в ответе за цифровой мир» [2] при поддержке Росмолодежи (2019 г.):

- около 70% молодых людей (15-25 лет) сталкивались с пропагандой экстремистско-террористической идеологии в интернет-среде и с призывами к несанкционированным действиям;
- около 60% молодежи получают информацию о способах самоубийства в сети интернет;
- более 70% сталкиваются с контентом о способах причинения себе физического вреда и боли.

Данное исследование отражает, насколько сеть Интернет наполнена деструктивной информацией. Однако до сих пор является актуальным вопрос о противодействии деструктивному воздействию. По данным опроса ВЦИОМ о цензуре в социальных сетях и об отношении россиян к ней (2021 г.):

- 51% россиян придерживаются мнения, что нужно блокировать любую недостоверную информацию в интернете;
- 23% считают, что нужно блокировать только ту недостоверную информацию, которая представляет серьезную угрозу;
- 14% придерживаются мнения, что блокировке должна подлежать даже потенциально вредная информация [3].

На данный момент проблема заключается в том, что электронные информационные ресурсы содержат большое количество деструктивной информации, которая оказывает негативное влияние на здоровье людей. Целью данной работы стало разработка метода противодействия деструктивному воздействию на личность.

## Анализ проблемы

Различные способы деструктивного воздействия существовали всегда, однако с началом развития сети Интернет их стало намного больше. Многие материалы деструктивной направленности, распространяющиеся в сети Интернет, отслеживаются на правовом уровне.

Отечественными нормами права предусматриваются запреты на распространение деструктивной информации и привлечение к юридической ответственности, в частности, о способах совершения самоубийства (ст. 110.2 УК РФ), клевете (ст. 128.1 УК РФ, ст. 5.61.1 КоАП РФ), террористической деятельности (ст. 205.2 УК РФ), ложной информации об обстоятельствах, представляющих угрозу жизни, здоровью и безопасности граждан либо повлекших тяжкие последствия (ст. 207.1 и 207.2 УК РФ), порнографических материалов (ст. 242, 242.1 УК РФ), материалов, возбуждающих ненависть или вражду (ст. 282 УК РФ), о наркотических средствах, психотропных веществах, их прекурсорах и т. п. (ст. 6.13 КоАП РФ), скрытой (завуалированной) вредоносной информации (ст. 13.15 КоАП РФ), демонстрирующей нацистскую символику и атрибутики (ст. 20.3 КоАП РФ) и др. [4; 5].

Несмотря на то, что указанные выше типы информации являются наиболее деструктивными, негативное влияние на личность могут оказывать еще несколько категорий информации. Благодаря анализу Регионального общественного центра интернет-технологий (РОЦИТ) были выделены девять категорий деструктивной информации [6], которая находится в серой зоне и на данный момент не регулируется уголовным или административным правом:

- контент, построенный на сексуализации несовершеннолетних;
- контент, популяризирующий проявления насилия в отношении людей;
- контент, популяризирующий самоповреждение;
- контент, популяризирующий насилие в отношении животных;
- контент, популяризирующий киберунижение;
- контент, популяризирующий оккультные услуги, направленные на причинение вреда жизни, здоровью, репутации и имуществу;
- контент, подрывающий нормы поведения в семье и школе;
- контент, популяризирующий нетрадиционные модели межполовых отношений, гендерной идентификации, доступный для несовершеннолетних или ориентированный на несовершеннолетних;
- ложная информация о пользе либо отсутствии вреда от употребления снюсов, вейпов, электронных сигарет и иных немедицинских заменителей табакосодержащей продукции.

Наибольшему влиянию деструктивной информации подвержена молодежь и подрастающее поколение из-за социально-возрастных и социально-психологических особенностей. «Порядка 13,5 миллиона подростков находятся под постоянным воздействием деструктивного контента в социальных сетях. Если мы не поставим эффективный заслон этому потоку грязи, то мы потеряем Россию как таковую. Через детей и подростков идут манипуляции, серьезная обработка политического характера», – указала глава Лиги безопасного интернета Екатерина Мизулина [6]. Следовательно, при разработке методов противодействия деструктивному воздействию в первую очередь необходимо ориентироваться на людей в возрасте от 14 до 25 лет, которые являются наиболее активными пользователями сети Интернет и потребляют наибольшее количество информации из электронных информационных ресурсов.

На данный момент существует несколько различных методов противодействия деструктивному воздействию. Основным методом решения данной проблемы является нормативно-правовое регулирование, которое затрагивалось ранее. Свод нормативно-правовых актов служит ограничителем субъектов деструктивного воздействия в их деяниях, а также устанавливает то, какие именно деяния будут являться преступными, указывает меру наказания за нарушение закона. Положительной стороной данного метода является тот факт, что нормативно-правовые акты одинаково действуют по всей стране и распространяются на каждого человека на ее территории. В них описаны все требования к организациям, юридическим и физическим лицам. Отрицательным фактором является необходимость постоянного обновления законодательства ввиду появления новых типов деструктивной информации и способов ее распространения.

Также существуют такие методы борьбы, как:

1) Ручное модерирование информации, распространяемой в социальных сетях. Данный метод потенциально обеспечивает качественную обработку нежелательной информации, однако является дорогостоящим и не быстродействующим процессом.

2) Автоматическое модерирование информации, распространяемой на различных сайтах и в социальных сетях. Скорость обработки информации данным методом в разы превышает скорость обработки при ручной модерации, однако в этом случае существует вероятность, что некоторое количество нежелательной информации останется незамеченным и необработанным.

3) Мониторинг различных интернет-ресурсов. Данный метод осуществляет блокировку сайтов, содержащих запрещенный контент, однако при этом требует большого периода времени ввиду того, что блокировка происходит только по решению суда.

4) Базовое обучение противодействию деструктивной информации в сети. Такое обучение преподносит основные понятия и способы защиты от психологического воздействия, однако качество обучения может зависеть не только от источника, но и от личности и ее восприятия.

5) Информирование пользователей о потенциально опасной информации. Информирование позволяет заблаговременно предупредить о том, что ресурс содержит нежелательную или запрещенную для некоторых категорий возрастов информацию. В данном случае такое информирование является только предупреждением, но никак не ограничивает личность от доступного контента.

6) Проверка сайтов через специальные ресурсы (Например, сайт довериевсети.рф). Подобные ресурсы предоставляют возможность посмотреть информацию о различных сайтах, убедиться в их надежности или ненадежности. Однако, очевидно, что не обо всех сайтах в сети Интернет найдется подобная информация на указанном ресурсе.

Определить единственный метод противодействия вредоносному влиянию, который в полной мере решал бы все проблемы одновременно, невозможно, так как различные методы деструктивного воздействия преследуют разные цели и имеют разные способы реализации. Следовательно, необходимо найти наиболее актуальный на данный момент метод противодействия деструктивному воздействию на личность.

**Актуальность разработки**

По нашему мнению, наиболее актуальным методом противодействия деструктивного воздействия на личность являются контент-фильтры. Контент-фильтр – это программа, которая блокирует доступ к веб-сайтам с содержимым, запрещенным для просмотра.

Рассмотрим наиболее популярные из них:

1) Akismet – это программа, которая фильтрует спам на блогах, форумах и других онлайн-платформах и использует алгоритмы машинного обучения для выявления нежелательных комментариев и сообщений.

2) Google SafeSearch – это программа, которая фильтрует контент для поисковой системы Google, которая блокирует нежелательный контент, включая порнографию и насилие.

3) Net Nanny – это контент-фильтр для родительского контроля, который помогает родителям контролировать доступ своих детей к нежелательному контенту в Интернете.

4) OpenDNS – это программа для провайдеров интернет-услуг, которая блокирует доступ к нежелательным сайтам и контенту для пользователей сети.

5) Sentiment Analysis API – это программа, которая использует анализ тональности текста для определения эмоциональной окраски сообщений и выявления негативных комментариев и отзывов.

Существует и другие подобные программы со своими положительными и отрицательными сторонами.

Контент-фильтры подразделяются на несколько типов. Один из наиболее распространенных – это установка программного обеспечения, которое блокирует доступ к вредоносным сайтам и фильтрует вредоносный контент. Это может быть полезно для тех, кто хочет ограничить доступ к определенным сайтам и контенту. Вторым типом является использование браузерных расширений, которые блокируют доступ к вредоносным сайтам и фильтруют вредоносный контент. Этот метод имеет некоторые преимущества перед установкой программного обеспечения, так как он может быть легко настроен и использован с любым браузером. Третий тип подобных программ – это инструменты для фильтрации деструктивной информации на уровне операционной системы, которые предоставляются некоторыми производителями операционных систем.

Все перечисленные контент-фильтры имеют один общий недостаток – ни один подобный контент-фильтр не может защитить пользователя от деструктивной информации на экране монитора в рамках других приложений.

Сейчас множество людей получают и обрабатывают информацию не только в сети Интернет, но и из сторонних электронных информационных ресурсов. Вышеперечисленные аналоги не имеют возможности модерировать и фильтровать всю информацию на экране пользователя, у них есть доступ лишь к определенному приложению или сайту.

Также в подобных контент-фильтрах актуальным остается вопрос безопасности данных. Любой пользователь желает, чтобы как можно меньше информации о нем обрабатывалось сторонними программами и куда-либо передавалось. Исходя из данных факторов можно сделать вывод о необходимости разработки программы контент-фильтра, у которой будет возможность блокировки любой деструктивной информации из различных источников на экране пользователя, а также возможность сохранения анонимности человека.

## Проект «Барьер»

В качестве решения проблемы деструктивного воздействия на личность нами предлагается проект «Барьер». Данный проект представляет из себя комплекс средств обнаружения вредоносной информации и ограничения ее воздействия на пользователя. Данная программа – это новый подход к борьбе с деструктивной информацией. Она обнаруживает деструктивную информацию, которая может вызывать негативное воздействие на зрительное восприятие и

психологическое здоровье пользователя, и выдает предупреждающее сообщение. При этом программа также скрывает информацию на экране, чтобы предотвратить ее воздействие на пользователя.

Для обнаружения деструктивной информации на экране монитора программа использует методы компьютерного зрения и алгоритмы обработки изображений.

Алгоритм работы программы включает в себя несколько этапов. Сначала программа делает снимок экрана монитора, затем она использует алгоритмы обнаружения символов для поиска текста на изображении. Далее программа проверяет найденный текст на наличие «запрещенных» слов, которые могут свидетельствовать о том, что на экране отображается деструктивная информация. Если такая информация была обнаружена, программа выдает информирующее сообщение, которое предупреждает пользователя о потенциальном вреде, связанном с деструктивной информацией.

Для того чтобы предотвратить воздействие такой информации на пользователя, программа скрывает ее на экране. Скрытие информации осуществляется с помощью специального алгоритма, который размывает область экрана, на котором была обнаружена деструктивная информация. Таким образом, пользователь не может распознать деструктивную информацию, что помогает ему избежать негативных последствий.

Программа также обладает рядом дополнительных возможностей, которые делают ее более эффективной и удобной для использования. Например, она настроена на работу в фоновом режиме, что позволяет пользователю не прерывать свою работу и не отвлекаться от текущих задач. Кроме того, пользователь может настроить параметры программы, такие как словарь «запрещенных» слов, необходимость «замыливания» найденной негативной информации и появления предупреждающего сообщения.

Функциональная часть программы не будет иметь возможности подключения к сети интернет и сохранению каких-либо личных данных пользователя. Изображение содержимого монитора будет использоваться только для анализа на устройстве пользователя без возможности сохранения. Данная особенность разработки позволяет обеспечить пользователя уверенностью в том, что программное обеспечение безопасно и не несет за собой никаких рисков.

Проект «Барьер» является эффективным инструментом для защиты здоровья и благополучия пользователей, которые могут быть подвержены негативному воздействию деструктивной информации. Программа является более актуальным, универсальным и безопасным решением проблемы деструктивного воздействия на личность в сравнении с существующими способами борьбы, упомянутыми ранее.

Для проверки эффективности созданной нами программы были проведены тесты на различных типах деструктивной информации. Тестирование работы программы проводилась при решении разных задач в различных приложениях. Результаты тестирования показали, что программа успешно обнаруживает и скрывает деструктивную информацию на экране монитора, что помогает пользователям избежать негативных последствий, связанных с такой информацией. Кроме того, предупреждающее сообщение, выдаваемое программой, является эффективным средством, которое предупреждает пользователей о возможных рисках, связанных с деструктивной информацией. Программа работает стабильно и не вызывает существенных задержек в работе компьютера. Также было выявлено, что программа не влияет на качество изображения на экране, кроме тех случаев, когда деструктивная информация была скрыта.

Таким образом нами был сделан вывод о том, что результаты тестирования подтверждают эффективность и целесообразность использования созданной программы для защиты здоровья и благополучия пользователей от деструктивной информации на экране монитора.

## Проблемные вопросы разработки

В ходе разработки проекта «Барьер» был встречен ряд проблемных моментов, которые являются направлениями для дальнейшего совершенствования описываемой программы:

- Осуществление мультиплатформенности. В настоящее время очень важна возможность использования системы на таких операционных системах, как Windows, Linux, macOS, Android, iOS.
- Выбор списка «запрещенных» слов. Важно составить список слов, которые будут считаться запрещенными и должны быть заблокированы. Это может вызвать проблемы с определением, какие слова должны быть включены, и какие нет, а также с оценкой контекста использования слова.
- Поддержка разных языков. Программа должна иметь возможность работы с различными языками и распознавать запрещенные слова в текстах на этих языках. Различия в грамматике и лексике между языками приводят к трудностям реализации поддержки разных языков.
- Неправомерное блокирование содержимого. Программа может ошибочно блокировать допустимое содержимое, которое содержит слова, похожие на запрещенные. Это может привести к проблемам с цензурой и ограничением свободы слова. Необходимо определять контекст использования слова, чтобы избежать ложных срабатываний. Это может вызвать трудности из-за многозначности слов и различных способов их использования в различных контекстах.

- Обход работы программы. Злоумышленники могут использовать различные способы обойти программу, такие как замена букв, использование синонимов или сленга. Это требует постоянного обновления программы, чтобы она могла распознавать новые способы обхода.
- Производительность. Программа должна обрабатывать большие объемы данных в режиме реального времени, что может привести к проблемам с производительностью и задержками в обработке контента.
- Конфиденциальность. Программа должна обрабатывать личные данные, такие как логи сессий и тексты сообщений, и при этом обеспечивать конфиденциальность этих данных. Сложность может возникнуть из-за потенциальных угроз безопасности и возможности несанкционированного доступа к данным.
- Обучение нейросети. Важно создать систему, определяющую значение слов и контекст. Для этого требуется сформировать большую корректную выборку и в будущем регулярно увеличивать и обновлять данные, посредством которых происходит обучение.

## Заключение

Существуют различные аналоги разработки системы для обнаружения деструктивного контента, каждый из которых может иметь свои преимущества и недостатки, и выбор определенного аналога зависит от требований и задач конкретного пользователя.

Разработанный проект «Барьер» по борьбе с деструктивной информацией представляет собой инновационный подход к решению этой проблемы, объединяющий в себе машинное обучение и анализ данных. Благодаря использованию современных технологий и методов программа позволяет эффективно выявлять и блокировать информацию, несущую потенциально негативные последствия для пользователей.

Разработка программного обеспечения для борьбы с деструктивной информацией является актуальной задачей, которая требует совместных усилий специалистов различных областей знаний.

## Список источников

1. Карнаушенко Л.В. Деструктивное информационно-психологическое воздействие на массовую аудиторию: правовые аспекты противодействия // Вестник КРУ МВД России. 2017. № 2 (36). URL: https://cyberleninka.ru/article/n/destruktivnoe-informatsionno-psihologicheskoe-vozdeystvie-na-massovuyu-auditoriyu-pravovye-aspekty-protivodeystviya (дата обращения: 01.04.2023)

2. Солдатова Г.У., Чигарькова С.В., Дренёва А.А., Илюхина С.Н. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. – М.: Когито-Центр, 2019. – 176 с.

3. Социальные сети и цензура: за и против [Электронный ресурс]: ВЦИОМ. 16 марта 2021 // https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-cenzura-za-i-protiv (дата обращения: 01.04.2023)

4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Доступ из СПС «Консультант Плюс».

5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ. Доступ из СПС «Консультант Плюс».

6. Эксперты выделили девять типов деструктивного контента в интернете [Электронный ресурс] 15 ноября 2022 // https://lenta.ru/news/2022/11/15/internet/ (дата обращения: 01.04.2023)

## COUNTERACTION TO DESTRUCTIVE INFLUENCE. PRO-PROJECT «BARRIER»

***A.A. Miklin, M.D. Dudarev, R.Z. Latypov, A.I. Soskin, V.Y. Nikitina, E.Yu. Nikitina, V.R. Akishin, N.D. Cherkasov***
Perm State National Research University

**Abstract.** The paper deals with the problem of destructive impact of information in electronic information resources. The relevance of the problem lies in the wide spread of destructive information and inefficiency of the existing ways of counteracting the destructive impact. The purpose of this research is to study the problem of destructive influence on personality and to develop a method of counteraction. The existing methods of counteracting destructive influence have been analyzed, as a result of which it has been revealed that most of the solutions are limited to content filtering or restricting access to certain sites. This article presents a new method of counteracting destructive influence. Project Barrier – is a program that allows to detect and hide destructive information on the monitor screen, as well as to warn users about possible risks associated with such information. The program is an effective tool to protect users' psycho- logical health from destructive influence. The results of testing showed that the program works stably and effectively detects and hides destructive information. Despite the considered problematic aspects of implementation, the program has a future with its further improvement.

**Keywords:** *destructive impact, destructive information, methods of counteraction, counteraction to destructive impact, content filters.*

# ИССЛЕДОВАНИЕ СВЯЗНОСТИ АККАУНТОВ, УЧАСТВУЮЩИХ В ИНФОРМАЦИОННЫХ АТАКАХ

***Я.Р. Мустакимова, Т.С. Посохина, А.Н. Рабчевский***

Пермский государственный национальный исследовательский университет,
ООО «Сеуслаб»

**Аннотация**. Информационная атака – спланированное, массированное информационное воздействие на объекты с целью формирования общественного мнения и поведения в соответствии с задачами организаторов атаки. Под объектами понимаются конкретные люди, общество в целом, а также государство. Основным элементом противодействия информационным атакам является их выявление. Разные исследователи используют для обнаружения информационных атак разные комбинации признаков информационных атак. Эти признаки не позволяют обнаружить информационные атаки на ранних стадиях, поэтому необходимо уметь выявлять дополнительные признаки, которые могли бы позволить максимально сократить срок обнаружения информационной атаки.

**Ключевые слова**: *информационная атака, признаки информационной атаки*.

## Введение

В современном мире социальные сети стали неотъемлемой частью повседневной жизни людей: они находят друзей в социальных сетях, общаются друг с другом, делятся своими мнениями, используют социальные сети для продвижения бизнеса и самовыражения. Социальные сети также являются эффективным средством для распространения информации. В социальных сетях можно найти актуальные новости и статьи, следить за текущими событиями. Благодаря широкому кругу контента, который публикуют пользователи, можно обогатить свои знания по интересующим вопросам. Но кроме полезной информации в социальных сетях можно встретить и деструктивную информацию, которую распространяют злоумышленники и различные преступные группировки. С помощью социальных сетей они пытаются манипулировать сознанием людей, изменять их убеждения и даже влиять на их поведение. В последнее время социальные сети все чаще используются для проведения информационных атак.

Словосочетание «информационная атака» впервые употребляется американскими военными специалистами в связи с формированием концепции информационной войны. Информационная атака – спланированное, массированное информационное воздействие на объекты с целью формирования общественного мнения и поведения в соответствии с задачами организаторов атаки [1]. Под объектами понимаются конкретные люди, общество в целом, а также государство. Основным элементом противодействия информационным атакам является их выявление. Разные исследователи используют для обнаружения информационных атак разные комбинации признаков информационных атак. Среди этих признаков можно выделить: увеличивающееся количество публи-

каций близкого по смыслу целевого контента, небольшой временной интервал между публикациями, стремление к максимальному охвату аудитории и др. [2]. Эти признаки не позволяют обнаружить информационные атаки на ранних стадиях, поэтому необходимо уметь выявлять дополнительные признаки, которые могли бы позволить максимально сократить срок обнаружения информационной атаки.

## Обзор литературы

Публикуемая в социальной сети информация должна быть правдивой и актуальной, в этом случае она является безопасной. Но во время информационных атак намеренно распространяются ложные новости. Это явление получило название дезинформация. Дезинформация – это искаженные или заведомо ложные сведения, распространяемые с целью пропаганды, с целью ввести информируемое лицо в заблуждение [3].

В 2020 году появился ещё один термин – дипфейк (deepfake). Дипфейк – это комбинация двух терминов: deep learning – глубинное обучение и fake – подделка. Дипфейк подразумевает максимальную маскировку ложной информации под правдивую с помощью методов искусственного интеллекта [4]. Выявить замаскированную ложную информацию по содержанию сложнее, чем явный деструктивный контент. Появление такого явления как дипфейки дает толчок к поиску новых способов обнаружения информационных атак без лексического анализа содержания контента. Одним из таких способов является анализ аккаунтов.

Взаимодействие аккаунтов отражают социологические модели представления социальных сетей. Описание подобных моделей иногда включает термин «информационные волны» (упрощенное представление информационных атак). Информационная волна – это управляемое распространение информации по целевым группам с целью достижения социального эффекта [5].

Моделирование процесса распространения информации невозможно без визуализации социальных связей между людьми, участвующих намеренно или случайно в информационных атаках. Визуализация связей используется в работе программы «The fake news graph analyzer (FNGA)», созданной в 2021 году [6]. Создатели программы поэтапно отлеживают с её помощью процесс распространения информации от одного пользователя социальной сети Twitter к другому. Алгоритм программы состоит из шести этапов:

- сбор информации о публикациях, сделанных влиятельными пользователями сети;
- выявление «нежелательных» распространителей информации, т.е. пользователей, часто публикующих деструктивный контент;
- построение графов (визуализация результатов предыдущих этапов);

- поиск взаимосвязей между авторами публикаций и пользователями социальной сети, разместившими копии публикаций на своих страницах. При этом учитываются публикации как с ложной, так и с правдивой информацией на одну тему;
- изучение характеристик графов распространения информации;
- определение центральности вершин графов.

Данный алгоритм детально разработан и хорошо подходит для анализа распространения информации в социальной сети Twitter.

Ученые из Греции [7] тоже моделировали взаимодействие пользователей социальной сети с помощью графов. Исследователи собирали следующие данные о первоначальном посте (исходной публикации) и всех репостах (копиях публикации):

- идентификатор пользователя, сделавшего пост;
- дату и время создания поста;
- основной текст поста или его репостов (это было необходимо для анализа содержания постов).

Собранную информацию ученые записывали в структуру diffusion tree – дерево распространения информации в социальной сети. Для каждого поста или репоста в дереве создавалась отдельная вершина. Цель построения структуры diffusion tree – поиск исходной публикации через поиск предшественника каждой из её копий. Вершины дерева хранили информацию о трех параметрах публикации: о связи с другими публикациями, о профиле пользователя, разместившего публикацию на странице в социальной сети, о вовлеченности пользователя и связанных с ним пользователей в распространении недостоверной информации.

С помощью деревьев ученые формировали временную последовательность публикации репостов, выявляли информационные треки и определяли вероятность принадлежности исследуемой совокупности публикаций к кампании по распространению дезинформации.

В исследовании учитывались дружеские связи между пользователями, но дерево строилось не как социальный граф. Действия ученых были направлены на построение графа публикаций от самой поздней во времени до исходной.

Программа для построения дерева была разработана для социальной сети Twitter. Как отмечают сами авторы программы: «программа не адаптирована для других социальных сетей».

Исследования зарубежных ученых направлены, конечно, не только на изучение социальной сети Twittter. Есть, например, работы о распространении ложных и правдивых видео на платформе YouTube [8], работы о дезинформации в сети Facebook [9].

Ранее вопросы распространения информации изучались маркетологами, и ими были сделаны значительные исследования в этой сфере. Например, была разработана модель SIPS [10].

Модель SIPS разделяет процесс распространения информации на четыре этапа:

- Sympathize – резонанс, информация о продукте находит отклик у потребителей;
- Identify – подтверждение, потребители анализируют, является ли информация о продукте ценной, собирают дополнительные данные;
- Participation – это участие, потребители совершают покупку;
- Sharing and spread – совместное использование и распространение, хороший потребительский опыт побуждает людей спонтанно делиться описанием покупок в социальных сетях и создавать вторичную рекламу.

Модель SIPS была разработана для онлайн-маркетинга продуктов, но деструктивный контент в информационных атаках тоже является своеобразным «продуктом», который распространяется в соответствии с маркетинговой стратегией. Следовательно, модель SIPS можно применить для объяснения поведения пользователей при распространении информации в социальных сетях.

Возможна следующая интерпретация модели SIPS по отношению к информационным атакам:

- Sympathize – быстрое распространение большого количества эмоциональных сообщений автоматическим способом, например, с помощью ботов;
- Identify – считывание информации пользователями (выражение реакции в виде лайков);
- Participation – пользователь анализирует информацию, определяет свое отношение к ней (комментарии);
- Sharing and spread – начало естественного распространения информации другим пользователям.

Три последних этапа можно выделить и в случае распространения достоверной информации в социальной сети. А первый этап характерен для информационной атаки. Он позволяет обозначить такие признаки информационной атаки, как массовый вброс информации, т.е. быстрое и обширное распространение информации с целью вызвать резонанс в обществе, и небольшой промежуток времени между первой и последней публикациями [11, 12]. Кроме того, характерным признаком первого этапа является использование автоматизированных способов внедрения информации, как правило с помощью ботов. При этом, крайне маловероятно, что большое количество незнакомых между собой людей естественным образом без общей цели и намерений будут одновременно публиковать идентичный контент. Такое поведение является показателем организованной деятельности инициаторов информационной атаки. Следовательно,

одним из признаков информационной атаки может быть использование независимых каналов для организации массового вброса целевого контента. Таким образом, актуальной является задача выявления социальных связей между аккаунтами, участвующими в одновременной публикации идентичного или близкого по смыслу контента.

## Постановка задачи

Целью данной работы является исследование использования независимых каналов вброса информации при проведении информационных атак. В качестве исследуемой социальной сети выбрана российская социальная сеть «ВКонтакте», в которой каналами распространения информации являются аккаунты, публикующие близкий по наполнению контент.

## Метод исследования

Было проведено исследование информационной атаки по теме «Дворец Путина», которая проходила в социальной сети ВКонтакте.

Процесс исследования информационной атаки состоял из следующих этапов:

- *Получение данных* об инфоповоде. Инфоповод – это поток сообщений, которые публикуют пользователи социальной сети, при этом все сообщения объединены одной тематикой [2]. Необходимо было получить список всех постов и репостов по теме инфоповода, идентификаторы пользователей, сделавших пост/репост, дату и время создания публикацию. Содержание контента в настоящем исследовании не анализировалось.
- *Разделение всех постов и репостов на информационные треки*. Информационные треки – это посты или репосты с идентичным контентом, отсортированные по времени публикации. Разделение публикаций на информационные треки было выполнено с помощью программы «Информационный трек-детектор» [13]. Информационная атака как правило содержит множество информационных треков. После запуска информационного трека контент обычно публикуется очень быстро большим количеством аккаунтов, т.е. происходит массовый вброс дубликатов [2]. Исследование проводилось на 11456 информационных треках, наиболее детально исследовались 5 треков с наибольшим числом опубликованных дубликатов.
- *Сбор информации о наличии связей* между пользователями. Для выявления таких связей была создана программа на языке Python. Анализ проводился по идентификаторам пользователей, которые являются ссылками на страницы аккаунтов в социальной сети ВКонтакте. Программа выгружает списки друзей для конкретных аккаунтов социальной сети, подсчитывает в каждом информационном треке: количество связей между первыми 10 аккаунтами, опубликовавшими контент, количество связей за 1 час и общее число связей в ин-

формационном треке. Все результаты записываются в сводную таблицу. Созданная программа применялась и на четвертом этапе, цель которого аналогична цели второго этапа.

- *Выявление общих друзей* у исследуемых аккаунтов, т.е. проверка наличия посредников, связывающих пользователей друг с другом.
- *Визуализация связей* между пользователями через построение одноколенного и двухколенного графа с учетом центральности вершин. Вершинами графа являются аккаунты, намеренно или случайно участвовавшие в информационной атаке. Визуализация графов была сделана с помощью библиотеки Matplotlib [14] для языка Python и с помощью программы Gephi [15].

## Результаты

Первый результат работы, наиболее общий и значимый из всех – это соотношение числа информационных треков с независимыми каналами распространения информации и других информационных треков. Как следует из диаграммы, представленной на рисунке 1, количество треков без связей значительно (в 25 раз) превышает число треков со связями. Это означает, что большая часть контента, вброшенная в процессе развития информационной атаки, распространяется не связанными между собой аккаунтами.

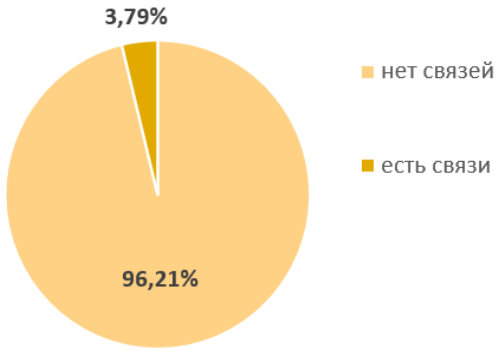



*Рис. 1. Наличие связей в информационных треках*

Диаграммы, представленные на рисунках 2 и 3, иллюстрируют распределение связей в различные промежутки времени. Соотношение информационных треков, в которых первые 10 аккаунтов, опубликовавших идентичный контент, не имеют прямых связей между собой, к общему числу информационных треков представлено на диаграмме, представленной на рисунке 2. Значение «0» означает, что связей между первыми 10 аккаунтами нет. Таких информационных треков – большинство (96%). Значение «100» означает, что количество связей между первыми 10 аккаунтами совпадает с общим числом связей. Такое соотношение характерно для треков с небольшим числом аккаунтов. Один процент от общего числа информационных треков составляют треки с другими

значениями соотношения, особенно с соотношениями 33% и 50%. Возможно, в подобных треках используются преимущественно естественные способы распространения информации. Тем не менее, в 96% случаев первые 10 публикаций идентичного контента были сделаны несвязанными между собой аккаунтами, что говорит об организованной целенаправленной деятельности по преднамеренному вбросу информации в социальную сеть.


*Рис. 2. Доли информационных треков с различным числом связей между первыми 10 аккаунтами, опубликовавшими контент*

На рис. 3 представлена диаграмма, которая отражает процентное соотношение числа связей между аккаунтами за 1 час и общего числа связей в информационных треках. Значения в легенде следует интерпретировать аналогично предыдущей диаграмме. Соотношение в 0% означает, что связей нет; 33% или 50% – треть или половина связей прослеживается в 1 час; 100% – после первого часа информационной атаки новые связи не появлялись, все связи объединяют активные аккаунты первого часа.


*Рис. 3. Доли информационных треков с различным числом связей между аккаунтами, опубликовавшими контент в течение часа после публикации первого поста*

Как следует из рис.3, в течение первого часа в 95% случаев идентичный контент публиковался пользователями, не имеющими прямых связей между собой. То есть распространение контента осуществлялось организованно. Далее с течением времени количество треков, имеющих связанные друг с другом аккаунты, увеличивается, что говорит о том, что распространение контента посте-

пенно становится более органичным и естественным. Такая динамика правдоподобна, потому что связанные друг с другом пользователи публикуют информацию не одновременно, а через некоторые случайные промежутки времени. В рассматриваемой совокупности информационных треков количество связей начинает увеличиваться спустя 45–60 минут после публикации первого поста.

В большинстве информационных треков количество независимых аккаунтов превышало количество аккаунтов со связями. Вероятно, в подобных треках изначально информация распространялась автоматически инициаторами информационной атаки. Естественное распространение начиналось только через определенный отрезок времени и было менее масштабным, чем автоматическое распространение информации.

Треки со значительным числом аккаунтов-участников (более 150) удачно подходят для изучения графов связей между аккаунтами. Двухколенные графы данных треков иллюстрируют противоположные варианты сценариев информационного трека. Первый сценарий – число независимых аккаунтов постоянно, общих друзей-посредников между пользователями нет. Второй сценарий – информационным треком управляют несколько главных аккаунтов. Они связаны с большинством аккаунтов, распространяющих новость. Главные аккаунты не публикуют контент сами, но заставляют другие аккаунты дублировать одну и ту же новость.

Добавление главных аккаунтов в качестве вершин в граф информационного трека кардинально изменяет структуру графа. Почти все аккаунты становятся связанными друг с другом через один общий узел. Это утверждение продемонстрировано на рисунках 4, 5 и 6.

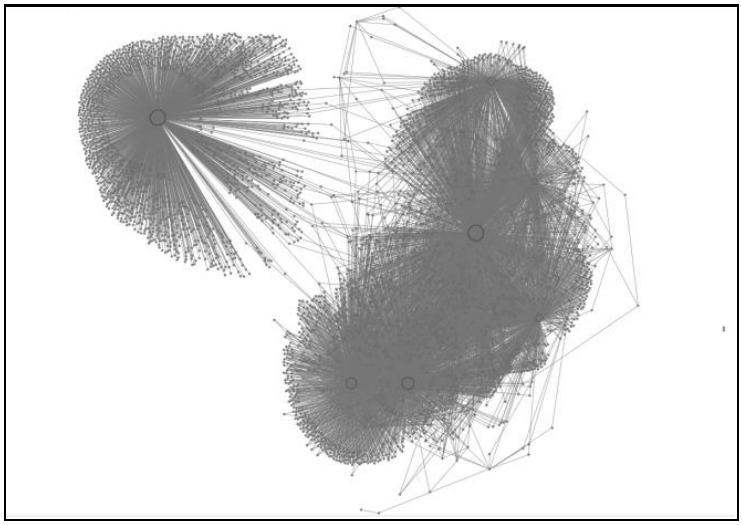


*Рис. 4. Изначально в информационном треке было 462 связей, после добавления посредников стало 7753 связей*

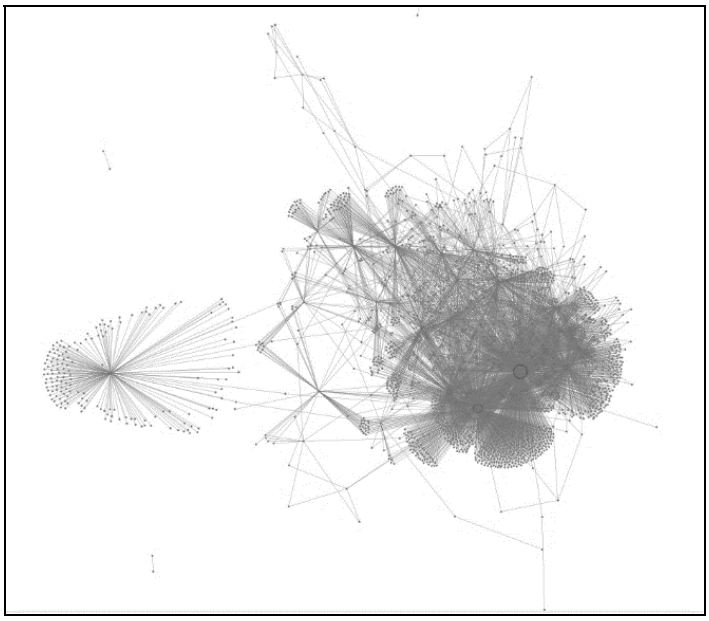


*Рис. 5. Изначально в информационном треке было 733 связей, после добавления посредников стало 5928 связей*

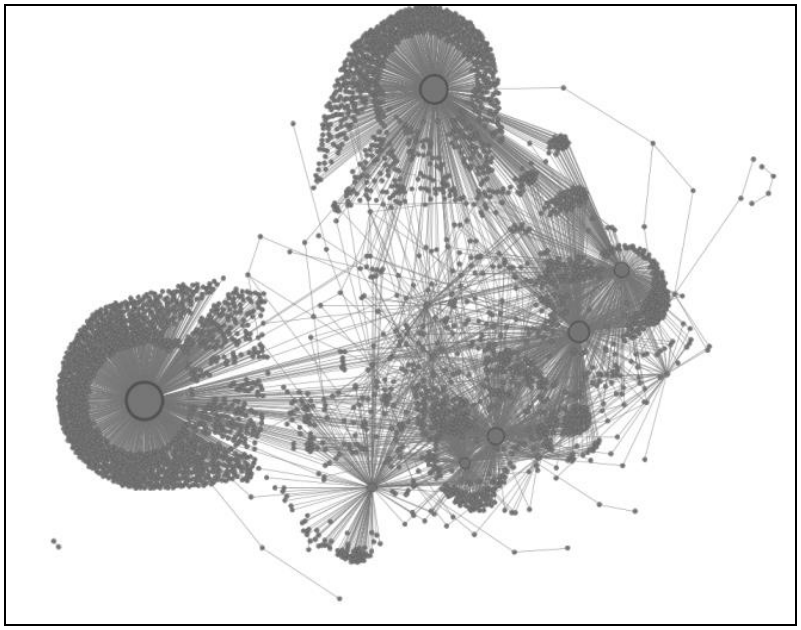


*Рис. 6. Изначально в информационном треке было 332 связей, после добавления посредников стало 4883 связей*

При построении графов были также выявлены информационные треки-исключения, процесс появления связей в которых отличался от остальных треков, где все аккаунты информационного трека были связаны между собой (рис. 7). Скорее всего это значит, что все эти пользователи действительно являются друзьями или связаны друг с другом общими интересами. И когда появилась определенная информация, они просто распространили её между собой.

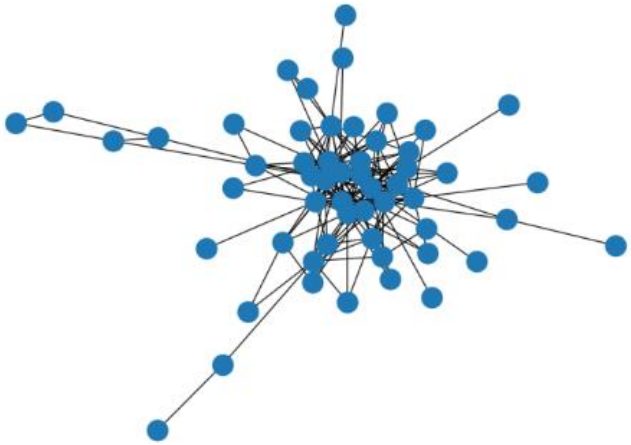


*Рис. 7. Все аккаунты, опубликовавшие контент, связаны между собой*

## Заключение

В результате проведенных исследований была изучена информационная атака по инфоповоду «Дворец Путина». В ходе исследования были получены убедительные свидетельства того, что массовый вброс идентичного контента осуществлялся в короткий промежуток времени через большое количество независимых каналов. При этом количество независимых каналов распространения информации значительно превышает количество каналов со связями. Исследование дополнительных связей показало, что аккаунты, через которые вбрасывался контент и которые на первый взгляд не связаны между собой, оказываются связаны с едиными центрами управления, что является дополнительным доказательством целенаправленной деятельности в процессе вброса контента. Таким образом, использование независимых каналов распространения информации можно считать явным признаком информационной атаки. Поскольку вброс целевого контента в виде дубликатов всегда происходит в начальной фазе развития информационной атаки, то анализируя связи между первичными каналами вброса контента, можно выявлять информационные атаки на их ранних стадиях. Выявление информационных атак на ранних стадиях развития может позволить более оперативно реагировать на информационные атаки и, таким образом, повысить эффективность противодействия этим атакам.

## Список литературы

1. Коцюбинская Л.В. Информационная атака: понятие и онтологические свойства // Политическая лингвистика. 2017. № 6. С. 106–111.

2. Минаев В.А., Рабчевский А.Н., Мустакимова Я.Р. Выявление информационных операций в социальных сетях на их ранних стадиях // Информация и безопасность. 2022. Т. 25. Вып. 4. С. 485–494.

3. Подход НАТО к противодействию дезинформации. [Электронный ресурс] URL: https://www.nato.int/cps/ru/natohq/topics_219728.htm (дата обращения: 05.12.2023)

4. Дипфейк. [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%BF%D1%84%D0%B5%D0%B9%D0%BA (дата обращения: 05.12.2023)

5. Градосельская Г.В., Щеглова Т.Е. Теоретические основы исследования информационных волн в социальных сетях // Управление развитием крупномасштабных систем MLSD'2019.: ИПУ РАН, 2019. С. 1196–1199.

6. Bodaghi A., Oliveira J., Zhu J. The fake news graph analyzer: An open-source software for characterizing spreaders in large diffusion graphs // Software Impacts. 2021. V. 10.

7. Michail D., Kanakaris N., Varlamis I. Detection of fake news campaigns using graph convolutional networks // International Journal of Information Management Data Insights. 2022. V. 2. No. 2.

8. Abul-Fottouh D., Song M., Gruzd A. Examining algorithmic biases in YouTube's recommendations of vaccine videos // International Journal of Medical Informatics. 2020. V. 140.

9. Guess A., Nagler J., Tucker J. Less than you think: Prevalence and predictors of fake news dissemination on Facebook // Science Advances. 2019. V. 5. No. 1.

10. Yang B., Zhang R., Cheng X., Zhao C. Exploring information dissemination effect on social media: an empirical investigation // Personal and Ubiquitous Computing. 2023. V. 27. P. 1469-1482.

11. Еременко В.Т., Рязанцев П.Н. Информационное противоборство в социотехнических системах. Орел: ОГУ им. И.С. Тургенева, 2016. 209 с.

12. Рабчевский А.Н., Карпов М.Ю., Ашихмин Е.Г. Выявление признаков информационных операций на основе анализа начальной частоты публикации дубликатов // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 82–88.

13. Программа «Информационный трек-детектор» свидетельство о регистрации программы для ЭВМ регистрационный № 2022668598 от 10.10.2022.

14. Matplotlib: Visualization with Python. [Электронный ресурс] URL: https://matplotlib.org/ (дата обращения: 05.12.2023)

15. Gephi – The Open Graph Viz Platform. [Электронный ресурс] URL: https://gephi.org/ (дата обращения: 05.12.2023)

## INVESTIGATING THE CONNECTIVITY OF ACCOUNTS INVOLVED IN INFORMATION ATTACKS

***Y.R. Mustakimova, T.S. Posokhina, A.N. Rabchevsky***
Perm State National Research University, LLC «Seuslab».

**Annotation.** Information attack is a planned, massive information impact on objects with the purpose of forming public opinion and behavior in accordance with the objectives of the attack organizers. The objects are understood as specific people, society as a whole, as well as the state. The main element of countering information attacks is their detection. Different researchers use different combinations of information attack signs to detect information attacks. These signs do not allow to detect information attacks at early stages, so it is necessary to be able to identify additional signs that could maximize the time of detection of information attacks.
**Keywords:** *information attack, signs of information attack.*

## ВЫЯВЛЕНИЕ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ НА ОСНОВЕ АНАЛИЗА ПАРАМЕТРОВ РАСПРОСТРАНЕНИЯ НЕЧЕТКИХ ДУБЛИКАТОВ

***Я.Р. Мустакимова, К.Л. Поторочина, А.Н. Рабчевский***
Пермский государственный национальный исследовательский университет, ООО «Сеуслаб»

**Аннотация**. В настоящее время основным источником отображения действительности становятся новые виды СМИ, такие как социальные сети, блоги, сайты и форумы. Для реализации информационно-психологического воздействия на пользователей различных социальных сетей внешние силы, представленные в виде отдельных государств, политических, экстремистских или террористических организаций, публикуют огромные потоки данных. Анализ массивов данных не представляется возможным без использования автоматизированных решений.
**Ключевые слова**: *информационная операция, векторизация текста, нечеткие дубликаты*.

### Введение

В настоящее время основным источником отображения действительности становятся новые виды СМИ, такие как социальные сети, блоги, сайты и форумы [1]. Они позволяют ускорить процесс распространения информации, поэтому активно используются для реализации информационных операций. Данное понятие, в работе [2], определяется как «действия, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информа-

ции и информационных систем и инфраструктуры». Для реализации информационно-психологического воздействия на пользователей различных социальных сетей внешние силы, представленные в виде отдельных государств, политических, экстремистских или террористических организаций, публикуют огромные потоки данных. Анализ массивов данных не представляется возможным без использования автоматизированных решений [3].

Информационные операции ведутся с целью дестабилизации общества и государства, то есть объектом воздействия является все население страны [4]. Обратимся к статистике ВЦИОМ 2021 года о медиа потреблении и активности в интернете. Для 21% россиян основным источником информации о новостях экономики и общественно-политической жизни страны и региона являлись социальные сети и блоги в интернете. Среди молодежи в возрасте от 18–24 и 25–34 лет этот процент еще выше (35–45%). По уровню доверия Интернет также занимает второе место после телевидения [5]. При этом половина россиян считает, что сможет отличить недостоверную информацию в интернете от достоверной [6]. Однако в работе [7] указывается, что на данный момент аудитория не может с точностью определить ложную информацию и сама становится ее распространителем. В статье также отмечается, что фейковая информация может быть синтезирована специальными ботами-программами, созданными для этой цели.

Таким образом, задача выявления информационных операций при помощи программных средств остается актуальной на данный момент и является элементом противодействия в информационной войне.

## Признаки и методы обнаружения информационных операций

Одним из способов проведения информационных операций в сети Интернет являются массовые вбросы, то есть распространение некоторой информации через множество источников [8]. Внедрение большого количества однотипных постов, появившихся в сети с высокой начальной частотой публикации, может считаться массовым вбросом, а, следовательно, и признаком информационной операции. В работе [9] отмечается, что временная метка создания поста может быть получена без задержки, а значит появляется возможность своевременно обнаруживать информационную операцию на основе создаваемых информационных треков. Информационные треки – это группы однотипных постов, отсортированных по времени публикации. Однако необходимо учитывать особенности совокупности таких публикаций. В работе [10] автор отмечает высокое подобие текстов сообщений, составляющих массовые вбросы. Такие схожие, но полностью не совпадающие тексты, называются нечеткими дубликатами [11]. Нечеткие дубликаты исходного текста могут быть получены путем

замены отдельных слов текста на синонимы, изменения словоформы (добавления суффиксов и приставок), добавления предлогов, частичной перестановки слов и т.д. В то же время точная копия исходного текста является четким дубликатом.

Наши исследования показали, что существует по меньшей мере два сценария проведения информационных операций. В основе первого сценария лежит массовый вброс большого количества четких дубликатов, целью которого является усиление эффекта широкой поддержки и актуальности некоторого инфоповода. В этом случае повторяющийся контент может иметь больше шансов попасть в топовые результаты поиска или вызвать реакцию большего числа пользователей. Однако использование абсолютно идентичных постов в информационной операции не всегда бывает успешным или незаметным. В другом сценарии используются нечеткие дубликаты. Информационные операции в таком случае становятся более сложными и многоуровневыми. Такой сценарий используется для запутывания и обмана алгоритмов фильтрации контента социальных сетей или поисковых систем. Следует отметить, что оба вида дубликатов могут одновременно использоваться для манипулирования общественным мнением.

## Постановка задачи

Чтобы в дальнейшем можно было анализировать информационные операции на предмет использования в них нечетких дубликатов, необходимо было научиться выявлять группы нечетких дубликатов в коллекции постов пользователей. Для этого нужно было выполнить следующие задачи:

– Изучить существующие методы векторизации текста. Под векторизацией текста понимается процесс конвертации текста в числа.

– Проанализировать разными методами тестовую выборку постов на наличие в ней групп нечетких дубликатов.

– Определить оптимальный метод для выявления групп нечетких дубликатов.

В предыдущих работах, уже был выполнен анализ начальной частоты публикации четких дубликатов [12]. Поэтому в данной работе необходимо было исследовать начальную частоту публикации групп нечетких дубликатов на основе коллекции постов пользователей из социальной сети ВКонтакте.

## Методика выявления групп нечетких дубликатов

### *Предварительная обработка*

Для реализации методов векторизации текста необходимо было произвести его предварительную обработку. Далее будут использоваться следующие термины:

*Корпус* – тестовая выборка всех постов по определенному инфоповоду.

*Документ* – отдельный пост пользователя, составляющий смысловую единицу.

*Токены* – текстовые единицы. В данном случае под токенами будем понимать слова, из которых состоит каждый документ.

Процесс предварительной обработки корпуса состоял из нескольких этапов:

1) Очистка корпуса от смайликов и набора «запрещенных» символов. К таким символам относятся: цифры, латинские буквы, знаки пунктуации и табуляции. Поскольку производится анализ русскоязычных постов, то из текстов были удалены все латинские буквы, следовательно, и ссылки на другие источники. Таким образом, посты, представленные в виде одной ссылки или набора ссылок, не связанных словами, исключались из рассмотрения и не допускались до этапа векторизации.

2) Удаление русских «стоп-слов». Список этих слов был взят из библиотеки NLTK. NLTK– это свободно распространяемая библиотека, которую можно использовать в приложениях для обработки естественного языка. В список «стоп-слов» вошли предлоги, союзы, частицы, междометия и другие части речи, которые часто встречаются в тексте, но смысловой нагрузки не несут. Всего в списке содержится 151 слово [13].

3) Перевод текста в нижний регистр. Данная операция позволяет увеличить число совпадающих токенов и облегчить сопоставление текстов.

4) Токенизация документов по словам. На данном этапе происходит преобразование непрерывной строки в структурированный набор, единицей которого является слово.

5) Лемматизация полученных токенов. Это процесс преобразования слова к его первоначальной форме. Глаголы приводятся к инфинитиву, существительные к единственному числу и именительному падежу и т.д. Для лемматизации использовалась библиотека pymorphy2. Это морфологический анализатор и генератор для русского и украинского языков, использующий словари из OpenCorpora[14].

6) Стемминг. Это процесс удаления частей слова для выделения его основы (удаление окончания, словообразовательных суффиксов и т.д.). Стемминг является более «грубой» операцией преобразования, чем лемматизация. В про-

цессе стемминга слово не приводится к своей первоначальной форме, а значит совпадающие по смыслу слова, могут быть заменены различными токенами. Поэтому стемминг выполняется после процесса лемматизации для сохранения числа совпадающих по смыслу слов. Для реализации стемминга использовался метод из библиотеки NLTK [13].

Таким образом, после предварительной обработки был получен очищенный корпус. Он состоял из документов – постов. Каждый из них был представлен в виде набора токенов – основной части значимых слов.

### *Методы векторизации*

Далее необходимо было провести векторизацию предварительно очищенного корпуса. В нашем исследовании использовались следующие методы:

- TF-IDF;
- Метод шинглов;
- Bag of word («мешок слов»);
- Transformers.

#### *TF-IDF*

Данный метод векторизации является одним из самых распространенных. Процесс получения векторов этим методом связан с подсчетом того, насколько часто токен встречается в документе (TF). При помощи TF оценивается важность токена в рамках конкретного документа.

$$TF(t,d) = \frac{n_i}{\sum_k n_k} \quad (1)$$

где $t$ – токен, $d$ – документ, $n_i$ – число вхождений токена в документ, $n_k$ – число всех токенов в документе.

На следующем этапе рассчитывается IDF, как инверсия частоты, с которой некоторое слово встречается в документах коллекции. Это позволяет понизить вес у широкоупотребляемых слов.

$$IDF(t,D) = \frac{|D|}{|(t_i \in d_i)|} \quad (2)$$

где $|D|$ – число всех документов коллекции; $|(t_i \in d_i)|$–число документов, в которых встречается токен $t_i$.

Итоговая мера TF-IDF представляется в виде произведения двух множителей TF и IDF [15].

$$TF - IDF = TF * IDF \quad (3)$$

*Метод шинглов*

В работе [11] говорится, что метод шинглов успешно применяется в анализе оригинальности контента веб-страниц и поиска плагиата. Поэтому мы также попробовали использовать данный метод для решения задачи поиска нечетких дубликатов.

Данный метод основан на разбиении текста на шинглы – последовательности подряд идущих слов. Они могут пересекаться или находиться отдельно друг от друга. Мы использовали деление на шинглы внахлест, через одно слово. Эти последовательности имеют фиксированную длину. Оптимальная длина составляет 3-10 слов. Чем меньше длина последовательности, тем точнее будет сравнение текстов и дольше процесс обработки. Для сравнения сходства текстов шинглы заменяются контрольными суммами, которые вычисляются с помощью различных алгоритмов хэширования.

После подсчета всех контрольных сумм нужно найти их пересечения. Чем больше пересечений у двух постов, тем выше степень их сходства.

*Bag of word («мешок слов»)*

В классическом виде «мешок слов» является одним из самых простых и популярных способов получения векторов из текстов. В данном методе сначала создается словарь уникальных слов в корпусе. После создается таблица, в которой столбцы соответствуют входящим в корпус уникальным словам, а строки – документам. Элементами таблицы будут числа, которые означают, сколько раз всего слово встретилось в документе. В данном методе не учитываются связи слов и их взаимное расположение. Принципиальным является лишь количество совпадающих слов. Если их достаточно много, то мы можем считать два текста нечеткими дубликатами. Однако, этот метод векторизации не лишен недостатков. В результате могут появиться векторы большой размерности и большой разреженности [16].

*Transformers*

Модель Transformers – это архитектура нейронной сети, которая получила широкое применение в области обработки естественного языка (Natural Language Processing, NLP) [17]. Transformers разработаны для решения задач, связанных с последовательностями данных, такими как тексты. Они позволяют обрабатывать и моделировать последовательности переменной длины, несмотря на их контекстуальную зависимость. Благодаря этому, Transformers превзошли предыдущие подходы, основанные на рекуррентных нейронных сетях (RNN), и стали основным инструментом в NLP. Например, в работе [18] языковая модель BERT, основанная на архитектуре Transformers, успешно использовалась для обнаружения поддельных новостей в социальных сетях.

### *Методы сравнения векторов*

Для сравнения векторов, полученных методами TF-IDF, Transformers и «мешок слов», мы использовали косинусное сходство. Эта мера изменяется в промежутке от 0 до 1. Для вычисления угла между векторами необходимо скалярно перемножить вектора и поделить на произведение длин рассматриваемых векторов. Для параллельных векторов, которые соответствуют абсолютно одинаковым текстам, косинус угла будет равен 1, а для перпендикулярных – 0 [15].

$$\cos\theta = \frac{A*B}{\|A\|*\|B\|} \quad (4)$$

где A, B – векторы.

Для выявления групп нечетких дубликатов необходимо было для каждого метода векторизации подбирать оптимальное пороговое значение косинусного сходства векторов. Если пара векторов, соответствующих некоторым постам, имела степень сходства выше порогового значения, то мы считали такие посты нечеткими дубликатами.

При работе с методом шинглов каждый документ представляется в виде контрольных сумм. Чем больше совпадающих контрольных сумм, тем более схожими считаются посты. Поэтому для сравнения значений, полученных данным методом, использовался подсчет совпадающих контрольных сумм в процентах.

### *Выявление групп нечетких дубликатов*

В данной работе в качестве тестовой выборки была взята коллекция постов из социальной сети ВКонтакте по инфоповоду «Специальная военная операция на Украине», содержащая 440 постов. В результате предварительного «ручного» анализа в данной выборке было выявлено 12 групп нечетких дубликатов. Эти группы считались эталонными.

При сравнении различных методов векторизации оценивались несколько параметров:

- количество найденных групп дубликатов, при условии, что в группу входит не менее 80% дубликатов, по сравнению с эталонной;
- средняя полнота групп в процентах, в сравнении с эталонной;
- время выполнения процедуры векторизации.

Метод TF-IDF был реализован при помощи библиотеки sklearn [19]. Полученные векторы сравнивались при помощи косинусного сходства. Оптимальное пороговое значение получилось равным 0,80. В лучшем случае, данный метод позволял найти 7 групп нечетких дубликатов из 12, а также предлагал

группу, которая нечеткими дубликатами не является. Это могло быть связано с тем, что нечеткие дубликаты, относящиеся к конкретному инфоповоду, представляли практически идентичные предложения, которые состоят из слов, имеющих равное значение. Время работы программы составило 18 секунд, а средняя полнота групп 96%.

При реализации метода шинглов для баланса скорости и точности длина шингла была выбрана равной 5. Для подсчета контрольных сумм использовался алгоритм хэширования CRC32 [20]. Для этого была подключена библиотека binascii [21], которая содержит в себе нужный алгоритм. Для сравнения использовался подсчет совпадающих контрольных сумм в процентах. Оптимальное пороговое значение составило 0,75. Результаты работы метода шинглов лучше, чем метода TF-IDF: было найдено большее число групп нечетких дубликатов, а также отсутствовали группы, которые ими не являются. Средняя полнота групп составила 98%, а время работы программы 14 секунд.

Метод «мешок слов» был реализован с помощью библиотеки sklearn. Сравнение полученных векторов осуществлялось методом косинусного сходства с пороговым значением равным 0,75. Данный метод оказался самым результативным, было найдено 11 групп нечетких дубликатов из 12, со средней полнотой 98%. Время работы программы составило 16 секунд.

При использовании Transformers важным вопросом является выбор подходящей модели. Мы использовали многоязыковую модель «distiluse-base-multilingual-cased-v1» [22], потому что она поддерживает русский язык. При использовании Transformers не требуется предварительной обработки текста, поскольку она выполняется автоматически. Имеется также встроенный метод для расчета косинусного сходства всех возможных пар векторов. Но пороговое значение, по которому определяется являются ли посты дубликатами, задавалось вручную. Оптимальное значение оказалось равным 0,89. Особенностью данного метода является то, что все группы, найденные этим способом, оказались полными (средняя полнота составила 100%). Нашлись недостающие посты, которые не были определены ни одним из реализованных выше методом. Однако при пороговом значении сходства в 0,89 не были найдены 3 группы нечетких дубликатов. Время работы данного метода на небольшой выборке составило 40 секунд.

В табл. 1 представлены сводные результаты поиска групп нечетких дубликатов по каждому из методов.

*Таблица 1*

*Сравнительная таблица*

| **Метод векторизации** | **Способ сравнения** | **Кол-во групп дубликатов** | **Средняя полнота групп** | **Время** | **Экспертная оценка** |
|---|---|---|---|---|---|
| Мешок слов | Косинусное сходство | 11 | 98% | 16 секунд | 9 |
| Transformers | Косинусное сходство | 9 | 100% | 40 секунд | 8 |
| Метод шинглов | Кол-во совпадающих контрольных сумм | 8 | 98% | 14 секунд | 7 |
| TF-IDF | Косинусное сходство | 7 | 96% | 18 секунд | 5 |

Если сравнить результаты работы всех методов, то можно сделать вывод, что лучший результат был получен методом векторизации «мешок слов» в сочетании с косинусным сходством.

### Метод выявления информационных операций

Для анализа наличия информационных операций в коллекции постов была применена программа «Информационный трек-детектор» [23]. Данная программа была модифицирована путем добавления в неё метода формирования групп нечетких дубликатов. В качестве метода векторизации для выявления нечетких дубликатов был использован «мешок слов», а в качестве метода сравнения – косинусное сходство. Модифицированная таким образом программа стала способна выявлять нечеткие дубликаты, сортируя их по времени публикации и объединяя в информационные треки. Также для каждого информационного трека производился анализ аномально высокой начальной частоты публикации нечетких дубликатов. Для проведения исследования была использована коллекция данных, связанная с инфоповодом «Специальная военная операция на Украине» из социальной сети ВКонтакте. Данная коллекция включает в себя 4630 постов пользователей. В процессе анализа были выделены существенные отличия в поведении некоторых информационных треков.

Результаты анализа представлялись в виде таблиц с нечеткими дубликатами, графика и сводной таблицы, которая содержит информацию о временном интервале, в течение которого были опубликованы первые 10 дубликатов, а также их общее количество.

На рис. 1 представлен сводный график, который отражает все информационные треки, содержащие группы найденных нечетких дубликатов. Числами на

графике обозначены информационные треки. Эти треки характеризуются высокой начальной частотой публикации и значительным охватом. Подробная информация о каждом выделенном треке представлена в сводной таблице 2.

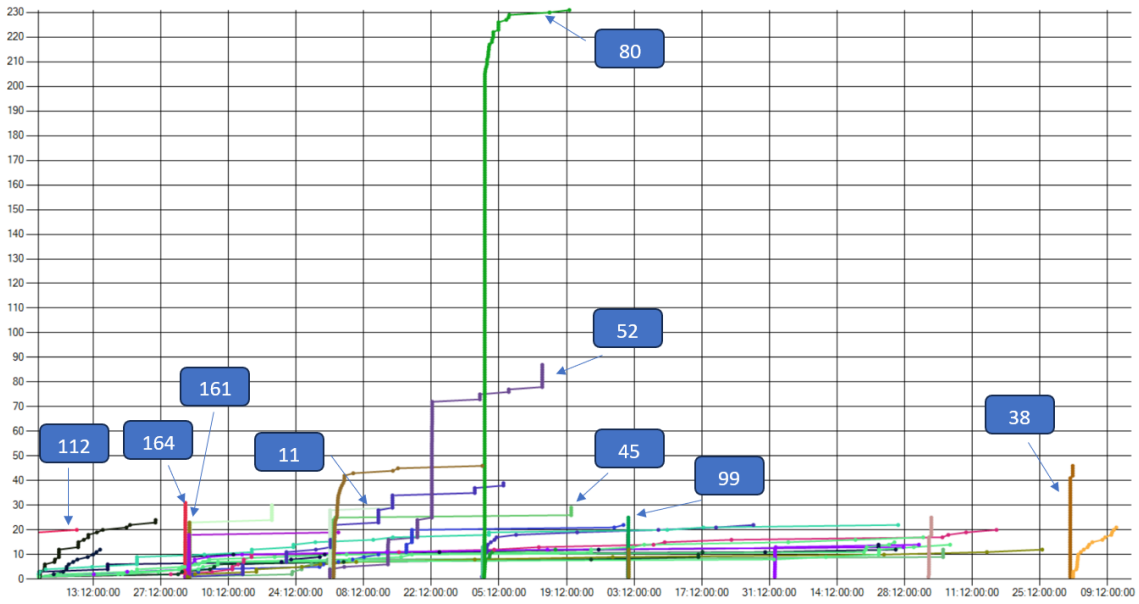



*Рис. 1. Сводный график по инфоповоду «Специальная военная операция на Украине»*

*Таблица 2*

*Информация о треках*

| **Номер трека** | **Общее количество дубликатов** | **Период публикации первых 10 дубликатов** |
|---|---|---|
| 80 | 231 | 0:02:44 |
| 52 | 82 | 0:28:30 |
| 38 | 46 | 0:04:57 |
| 11 | 34 | 0:13:23 |
| 164 | 31 | 0:05:39 |
| 45 | 29 | 0:02:08 |
| 99 | 25 | 0:08:47 |
| 161 | 23 | 0:02:48 |
| 112 | 20 | 0:01:36 |

Наиболее значимыми являются треки, в которых общее количество нечетких дубликатов превышает 20, а период публикации первых 10 дубликатов составляет менее 40 минут. Замечено, что в большинстве случаев этот период составляет всего несколько минут, что свидетельствует о преднамеренном массовом вбросе определенного вида контента. Например, в треке 80 первые 10 дубликатов были опубликованы в течение 2 минут, а их общее число достигло 231, что указывает на широкий охват.

Таким образом, результаты анализа сводного графика позволяют выявить информационные треки, характеризующиеся высокой начальной частотой и массовостью публикации нечетких дубликатов, что может свидетельствовать о проведении информационной операции с целью манипуляции данными и их широкого распространения. Дальнейшее исследование этих треков может помочь в раскрытии методов и мотиваций заинтересованных сторон и способствовать разработке мер по противодействию таким информационным операциям.

## Заключение

В проведенной работе была проанализирована коллекция постов пользователей на предмет наличия информационных операций. В качестве признака проведения операции был предложен метод анализа начальной частоты публикации нечетких дубликатов. Для обнаружения схожих, но не совпадающих полностью текстов был произведен сравнительный анализ методов векторизации текстов и методов сравнения полученных векторов. Наилучшее результаты показало сочетание векторизации методом «мешок слов» и сравнения векторов методом косинусного сходства. Предложенный метод позволяет выявить информационную операцию на ранней стадии, а обнаружение массовых вбросов нечетких дубликатов позволяет расширить спектр выявляемых операций, повысить гибкость поиска, а также учесть вариативность данных, возникающую из-за незначительных изменений. Сокращение времени обнаружения информационных операций позволит в короткие сроки принимать меры по предотвращению распространения вредоносной информации и ограничивать ее воздействие на пользователей социальных сетей и общество в целом.

## Список литературы

1. Расторгуев С.П., Литвиненко М.В. Информационные операции в сети Интернет / под. общ. ред. А.Б. Михайловского. М.: АНО «Центр стратегических оценок и прогнозов», 2014. 128 с.

2. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: монография. СПб.: Наукоемкие технологии, 2017. 546 с.

3. Савва Ю.Б. Автоматизация выявления деструктивного информационно-психологического воздействия на участников виртуальных социальных сетей // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран: сборник научных статей VIII Международной научно-практической интернет-конференции, Могилев, 15 марта – 15 апреля 2019 года

/ под ред. И.Н. Шарухо, А.В. Клебанова. – Могилев: МГУ имени А.А. Кулешова, 2019. С. 99-102.

4. Концепция Конвенции ООН об обеспечении международной информационной безопасности. [Электронный ресурс] URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 05.12.2023)

5. Медиапотребление и активность в интернете. [Электронный ресурс] URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/mediapotreblenie-i-aktivnost-v-internete (дата обращения: 05.12.2023)

6. Социальные сети и цензура: за и против. [Электронный ресурс] URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-cenzura-za-i-protiv (дата обращения: 05.12.2023)

7. Родионова Е.М. Маркеры фейковой информации и способы их выявления // Трибуна ученого. 2022. № 5. С. 391-398.

8. Столбов А.А. Концепция сетевой войны в современном мире // Школа Науки. 2018. № 2(2). С. 67-68.

9. Kotteti C., Dong X., Qian L. Ensemble Deep Learning on Time-Series Representation of Tweets for Rumor Detection in Social Media. // Applied Sciences. 2020. V. 10.

10. Потемкин А.В. Распознавание информационных операций средств массовой информации сети Интернет // Интернет-журнал «Науковедение». 2015. Т. 7. № 3.

11. Загорулько Ю.А., Саломатина Н.В., Серый А.С., Сидорова Е.А., Шестаков В.К. Выявление нечетких дубликатов при автоматическом формировании тематических коллекций документов на основе web-публикаций // Вестник НГУ. Серия: Информационные технологии. 2013. Т. 11. № 4. С. 59-70.

12. Рабчевский А.Н., Карпов М.Ю., Ашихмин Е.Г. Выявление признаков информационных операций на основе анализа начальной частоты публикации дубликатов // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 82-88.

13. Natural Language Toolkit. [Электронный ресурс] URL: https://www.nltk.org/ (дата обращения: 05.12.2023)

14. Korobov M. Morphological Analyzer and Generator for Russian and Ukrainian Languages // AIST 2015: Analysis of Images, Social Networks and Texts. 2015. P. 320-332.

15. Валиев А.И., Лысенкова С.А. Применение методов машинного обучения для автоматизации процесса анализа содержания текста // Вестник кибернетики. 2021. №4 (44). С. 12-15.

16. Нугуманова А.Б., Бессмертный И.А., Пецина П., Байбурин Е.М. Обогащение модели Bag-of-words семантическими связями для повышения качества классификации текстов предметной области // Программные продукты и системы. 2016. №2. С. 89-99.

17. Gillioz A., Casas J., Mugellini E., Abou Khaled O. Overview of the Transformer-based Models for NLP Tasks // Proceedings of the 2020 Federated Conference on Computer Science and Information Systems. 2020. P. 179-183.

18. Kaliyar R.K., Goswami A., Narang, P. FakeBERT: Fake news detection in social media with a BERT-based deep learning approach // Multimedia Tools and Applications. 2021. V. 80. I. 8. P. 11765-11788.

19. Scikit-learn. Machine Learning in Python. [Электронный ресурс] URL: https://scikit-learn.org/stable/ (дата обращения: 05.12.2023)

20. Мальчуков А.Н., Осокин А.Н. Быстрое вычисление контрольной суммы CRC: Таблица против матрицы // Прикладная информатика. 2010. №2. С. 58-63.

21. Binascii – Convert between binary and ASCII. [Электронный ресурс] URL: https://docs.python.org/3/library/binascii.html (дата обращения: 05.12.2023)

22. Sentence transformers. Distiluse-base-multilingual-cased-v. [Электронный ресурс] URL: https://huggingface.co/sentence-transformers/distiluse-base-multilingual-cased-v1(дата обращения: 05.12.2023)

23. Программа «Информационный трек-детектор» свидетельство о регистрации программы для ЭВМ регистрационный № 2022668598 от 10.10.2022.

## IDENTIFICATION OF INFORMATION OPERATIONS ON THE BASIS OF FUZZY DUPLICATE PROPAGATION PARAMETERS ANALYSIS.

***Y.R. Mustakimova, K.L. Potorochina, A.N. Rabchevsky***

Perm State National Research University, LLC «Seuslab».

**Annotation.** Nowadays new types of mass media such as social networks, blogs, websites and forums are becoming the main source of reality display. To realize information-psychological impact on users of various social networks, external forces represented in the form of individual states, political, extremist or terrorist organizations publish huge data streams. Analysis of data arrays is not possible without the use of automated solutions.

**Keywords:** *information operation, text vectorization, fuzzy duplicates.*

# ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ УДАЛЁННОЙ РАБОТЫ СОТРУДНИКОВ

***М.О. Пьянков, Е.Ю. Никитина***
Пермский государственный национальный исследовательский университет

**Аннотация**. В данной статье рассматриваются такие вопросы как: актуальность информационной безопасности на удалёнке, факторы повышения уязвимости при работе из дома, цели злоумышленников и инструменты, с помощью которых они получают несанкционированный доступ. Какие конкретно действия сотрудников приводят к потере информации, а также размеры выкупов, которые платят компании, ставшие жертвой злоумышленников.
**Ключевые слова***: информационная безопасность; удалённая работа; уязвимости*.

За последние два года стало вполне очевидным, что в любой момент могут произойти непредсказуемые события, которые заставят почти всё население земли поменять свой привычный образ жизни. Примером тому является пандемия коронавируса 2020–2022 гг. Эпидемия коснулась всех сфер жизни, включая спорт, образование, покупки, транспорт, отдых, общественную жизнь, а также экономическую сферу.

Возникшие проблемы заставили работодателей менять условия труда. Возникла необходимость переводить большую часть работников на удалённый вид работы. Онлайн-собрания, обмен файлами, программное обеспечение для управления проектами, мгновенное обращение к работникам через мессенджеры и многие другие удобные инструменты были использованы для организации работы коллективов. У сотрудников пропала необходимость добираться до места работы, произошло снижение расходов организаций на содержание офиса. Всё это очевидные преимущества такого вида работы.

Несмотря на то, что с начала массового перехода на удаленную работу и прошло два года, проблемы, связанные с информационной безопасностью компании, остались.

Согласно ТК РФ Статье 312.1, дистанционной работой является выполнение, определённое трудовым договором, трудовой функции вне места нахождения работодателя, его филиала, представительства, иного обособленного структурного подразделения, вне стационарного рабочего места, территории или объекта, прямо или косвенно находящихся под контролем работодателя, при условии использования для выполнения данной трудовой функции и для осуществления взаимодействия между работодателем и работником по вопросам, связанным с её выполнением, информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей связей общего пользования.

Таким образом очевидно, что какая-то часть корпоративной информации будет передаваться через сети общего пользования, в том числе и интернет. Этот факт был неоднократно подтвержден практикой работы организаций в период пандемии. [3]

**Факторы повышения уязвимости информации**

Первый фактор, который сыграл наиболее важную роль, является фактор скорости перехода на удаленный режим работы.

Для большинства компаний работы были выведены из периметра защиты организации. В тот момент главной целью было восстановить работоспособность компании. Некоторые компании, к сожалению, впервые вспомнили про информационную безопасность, поскольку с первоначальной установки и настройки информационной сети в большинстве случаев никакие действия не производятся. Большинство руководителей не вспомнили про фактор информационной безопасности, поскольку он является не самым очевидным. Кроме того, в короткие сроки массового перехода на удаленный режим почти невозможно и очень дорого обеспечить сотрудников информационными и техническими ресурсами, которые помогли бы обеспечить должный уровень безопасности.

Вторым фактором является домашняя обстановка. В домашних условиях сотрудник менее бдителен, он слабо контролируем. Множество факторов в совокупности ослабляют внимание, остроту ума, пропадает должная осторожность при обращении с информацией.

Третьим фактором является персональный компьютер, который используется для обработки информации. Зачастую он является личным устройством сотрудника. Из этого вытекают следующие под факторы:

Подобный компьютер как правило является машиной, которой пользуется вся семья. В таких условиях к информации, обрабатываемой на этом компьютере, будут иметь доступ посторонние люди – с точки зрения компании это также создаёт определённые риски.

На личном компьютере крайне сложно контролировать устанавливаемое программное обеспечение, которое в свою очередь может быть заражено. Кроме того, на этом компьютере часто отсутствует должный уровень защиты.

Четвёртым фактором являются сами сотрудники компании. В условиях удаленного доступа отсутствует должный контроль за сотрудником. В силу этого сам сотрудник может передавать информацию злоумышленникам или сохранять её на собственных носителях, а потом использовать в личных целях.

Пятый фактор – ответственность за безопасность информации лежит полностью на сотруднике. К сожалению, сотрудника дома ничего не ограничи-

вает. Отсутствуют системы информационной безопасности, которые могли бы подстраховать сотрудника от вредоносных действий. [5]

## Примеры нарушения информационной безопасности в условиях удаленной работы

Пример 1. Организация удалённых совещаний. В силу неграмотности модераторов, не редки случаи присутствия посторонних гостей на совещаниях, что приводит к утечке важной информации. Имеется множество фактов, свидетельствующих о том, что в целях экономии компании пользовались триальными, демо версиями сервисов для проведения онлайн-мероприятий. Подобные программы включают в свой состав только простейшие функции по обеспечению вопросов безопасности.

Пример 2. Обработка и обмен информацией между сотрудниками. Использование в рабочих целях сторонних, открытых приложений, сайтов (мессенджеры, редакторы, облака) также повышает риски нарушения безопасности, так как зачастую их создатели являются неизвестными разработчиками, либо доступ к этим сервисам от лица пользователя слабо защищён.

Пример 3. Отсутствие информационной гигиены у сотрудников. Рядовым явлением в поведении сотрудников является оставление файлов с рабочей информацией открытыми на экране монитора; демонстрация экрана во время онлайн-меброприятий; открытые вкладки браузера; использование стандартных учётных записей и паролей низкого уровня сложности и т.д. Не стоит забывать о том, что инструменты, которые на первый взгляд упрощают жизнь, в свою очередь повышают уязвимость.

Пример 4. Нет ничего более постоянного, чем временное. В эту категорию входят все решения, сделанные в условиях спешки: плохая настройка информационной системы; отсутствие мультифакторной аутентификации, распределение пользователям получили большего количества полномочий, чем требуется и т.д.

Пример 5. Разрешение удалённого подключения к информационной системе. В условиях удаленного подключения требуется дополнительная защита для входа в информационную систему: биометрия, электронные ключи и прочее. На практике применение подобных инструментов встречается нечасто и, в первую очередь, в силу дороговизны требуемых средств. [2]

## Способы взлома, несанкционированного доступа

*Фишинг.* Это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Злоумышленники зачастую покупают базу данных электронных ящиков пользователей и начи-

нают массовую рассылку писем от имени известных фирм, брендов, банков, так же не редким исключением может быть ориентированная рассылка от имени руководителя вашей компании, из отдела кадров или вообще от генерального директора.

Во время коронавирусной инфекции было очень популярно отправлять заражённые письма от имени ВОЗ, различных ведомств и министерств здравоохранения. В этих письмах присутствуют заражённые ссылки, вложения, взаимодействия с которыми ведёт к утечке конфиденциальных данных.

По данным отчёта фирмы по кибербезопасности Norton каждое двухтысячное письмо является фишинговым, следовательно ежедневно совершается порядка 135 миллионов атак. Если сотрудники компании не могут распознать признаки фишинга, то под угрозой находится вся организация. По данным исследования Verizon, среднее время, необходимое первой жертве широкомасштабной фишинговой рассылки, чтобы открыть вредоносное письмо, составило 16 минут, а отдел ИБ узнаёт о фишинговой кампании только через 33 минуты. Учитывая то, что фишинг – это самый успешный и опасный вид кибератаки, так как 91 процент всех кибератак начинаются с фишинговой электронной почты, то за 17 минут вашу компанию могут настичь последствия, которые приведут к катастрофе. [4]

*Вредоносное программное обеспечение.* Существует 3 основных способа заражения компьютера удаленного пользователя: социальная инженерия, заражение системы без ведома пользователя, а также комбинация обоих методов.

Что касательно социальной инженерии, в этот способ входит злободневный фишинг (почта, сайты и т.д.), Malvertising (реклама на сайтах) P2P-сети (одноранговые). Обычно файлы в таких сообщениях имеют очень привлекательные имена: PasswordHacker.exe, MicrosoftCDKeyGenerator.exe, PlayStationemulatorcrack.exe. Например очень популярным способом во время локдауна было создание клонов-сайтов и приложения Zoom. Вторым способ получения вредоносного программного обеспечения является эксплуатация мошенниками уязвимостей в системах. Уязвимость – это брешь в коде или логике работы в операционной системе или прикладном программном обеспечении. Современные операционные системы и приложения достаточно сложны, имеют широкий функционал, в следствие этого разработчикам сложно создать программное обеспечение, которое не содержало бы никаких ошибок. Третий способ просто совмещает эти методы, делая его ещё более эффективным в силу сочетания массовости и сложности обнаружения: руткитов (rootkit), бэкдор (backdoor), ransomware (шифровальщики, блокировщики). [7]

*Взлом роутеров.* Причиной этому может стать отказ от смены пароля администратора после покупки (речь идёт не о наборе символов, который вы вво-

дите при подключении к Wi-Fi, а о пароле, который нужен для входа в панель настроек самого роутера). Второй причиной может послужить наличие брешей в прошивках. [9]

### Масштабы воздействий киберпреступников в связи с переходом на удаленный режим работы сотрудников

За 2021–2022 гг. главной угрозой безопасности для большинства компаний являлись операторы программ – вымогателей. По данным Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB, количество атак на организации на территории России в 2021 году увеличилось более чем на 200%. В России прослеживаются те же тренды, что и во всем мире – наиболее популярным способом проникновения в сетевые инфраструктуры организаций является компрометация публично доступных терминальных серверов (RDP (remote desktop protocol) – уязвимость, позволяющая удалённому пользователю скомпрометировать целевую систему). На них пришлось 60% всех расследованных атак. На фишинговые рассылки, где первичным вектором проникновения атакующих в сеть стала электронная почта, пришлось 22%, на эксплуатацию публично доступных приложений 14%, на иные методы – 4%. Размер запрашиваемого у российских компаний выкупа значительно варьируется и зависит от величины организации. Он колеблется от нескольких десятков тысяч до сотен миллионов рублей. Максимальной суммой первоначального выкупа является цифра в 40 миллионов рублей, а максимально запрошенный выкуп операторами программ-вымогателей составил 250 миллионов рублей. В 2020–2021 годах наиболее активными на территории России были операторы следующих программ-вымогателей: Dharma, Crylock, Thanos. С использованием каждой из программ было совершено более 100 атак.

Тренд на использования массовых фишинговых рассылок для получения изначального доступа к корпоративным сетям в 2021 году добрался и до России. Например, русская группировка OldGremlin за время своего существования успела совершить несколько успешных атак, а в некоторых случаях размер выплаченного выкупа достигал 40 миллионов рублей.

В зоне особого внимания хакеров находятся поставщики услуг и сервисов. В 2020 году было совершено около 200 атак на энергетические и промышленные компании, в то время как годом ранее их было 100. [6]

К сожалению информация, касающаяся точных данных о пострадавших, является либо закрытой, либо вообще недоступна в силу того, что ни одна компания не хочет, чтобы общественность была в курсе атак на неё, поскольку это негативно повлияет на инвестиции, репутацию, акционерное общество и т.д.

Несмотря на распространённое в обществе заблуждение, Россия активно подвергается кибератакам, а в условиях дистанционной работы риски повышаются в несколько раз.

В последнее время в информационной безопасности произошло частичное изменение целей обеспечения вопросов безопасности. Ранее одной из главных целей считалось определение границ защиты и построение системы защиты исходя их этих границ. На данный момент целью обозначается быстрое обнаружение злоумышленников внутри системы. Это связано с пониманием факта того, что невозможно создать абсолютно надежную систему защиты. Соответственно, новая цель заключается в том, чтобы не дать хакеру нанести серьёзный урон работе компании.

**Возможные пути решения**

На сегодняшний день уже существуют готовые решения и рекомендации для предприятий, которые защищают сотрудников от большинства уязвимостей. Согласно требованиям безопасности для государственных информационных систем, сотрудникам организаций, у которых есть доступ к закрытой служебной информации, запрещается работать с личных персональных компьютеров. Недавно ФСТЭК все же разрешила работу с конфиденциальной информацией на личных персональных компьютерах при условии использования сертифицированных средств защиты. Для этого предлагается использовать решение на базе технологии Live USB с защищённым хранилищем внутри и своей ОС. [12]

Live USB – это портативное внешнее устройство хранения данных, подключенное к USB, содержащее полную ОС, с которой можно осуществить загрузку компьютера. Live USB обеспечивают дополнительное преимущество повышенной конфиденциальности, поскольку пользователи могут легко носить USB-устройство с собой или хранить его в безопасном месте, уменьшая возможности для других лиц получить доступ к их данным. С другой стороны, USB-устройство легко потерять или украсть, поэтому шифрование и резервное копирование данных даже важнее, чем в обычной настольной системе.

Так же ФСТЭК были выпущены рекомендации для операторов объектов критической информационной инфраструктуры по обеспечению дистанционного режима работы сотрудников. Регулятор рекомендовал выделить удаленных работников в отдельный домен, включить для них двухфакторную аутентификацию и использовать на их рабочих местах средства криптографической защиты информации (VPN-клиент). Также ФСТЭК рекомендовал идентифицировать удаленные персональные компьютеры по MAC-адресам и предоставлять им доступ к внутренним ресурсам методом «белого списка». [13]

ФСТЭК информирует о недопустимости использования удаленного доступа для управления промышленным оборудованием автоматизированных си-

стем управления, которые при категорировании были отнесены к значимым объектам критической информационной инфраструктуры. Предложенные регулятором рекомендации включают в себя технические и организационные меры. Главным образом они направлены на контроль доступа к объектам (двухфакторная аутентификация, разграничение прав доступа и т.п.) и комплексную защиту задействованных каналов связи и конечных узлов сети (использование антивирусных решений, VPN, мониторинг безопасности).

Рекомендации Национального координационного центра по компьютерным инцидентам (НКЦКИ) во многом схожи с рекомендациями ФСТЭК России и содержат ряд дополнительных технических мер, включая сегментирование сети и контроль за подключением внешних носителей, а также отдельные меры по противодействию угрозам, связанных с мошенничеством.

И ФСТЭК России, и НКЦКИ говорят о необходимости проведения инструктажа персонала по вопросам безопасной удаленной работы, в том числе информирования о фишинговых атаках. [11]

## Заключение

Выполнение хотя бы половины всех вышеперечисленных рекомендаций снизит риски стать жертвой злоумышленников в разы. К счастью, большинство рекомендаций, предлагаемые авторитетными источниками не требуют больших финансовых вложений, следовательно осталось лишь донести до руководств компаний то, что они их безразличие или снисходительное отношение к этому вопросу лишь только привлекает злоумышленников, а это уже ведёт к серьёзным финансовым и репутационным проблемам.

## Список литературы

1. Бирюков А.В., Зиновьева Е.С., Зинченко А.В., Крутских А.В., Смирнов А.И. Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для вузов. 2-е издание Москва: Издательство «Аспект Пресс», 2021. – 384 с

2. Оливер Ибе Компьютерные сети и службы удалённого доступа Саратов: Профобразование, 2019. – 335 с.

3. Информационный веб-сайт «Трудовой Кодекс Российской Федерации». ТК РФ Статья 312.1 URL: https://www.trudkod.ru/chast-4/razdel-12/glava-49-1/st-312-1-tk-rf (Дата обращения: 12.06.2022)

4. [Электронный ресурс] Европейский информационный сайт-журнал по информационной безопасности MetaCompliance URL: https://www.metacompliance.com/ (Дата обращения: 10.03.2022)

5. [Электронный ресурс] Информационный веб-сайт Habr, связанный с информационными технологиями, бизнесом и интернетом URL: https://habr.com/ru/all/ (Дата обращения: 12.03.2022)

6. [Электронный ресурс] Информационный веб-сайт компании Group-IB URL: https://www.group-ib.ru/ (Дата обращения: 13.03.2022)

7. [Электронный ресурс] Информационный портал tadviser URL: https://www.tadviser.ru/ (Дата обращения:14.03.2022)

8. [Электронный ресурс] Обзор компании Group-IB «Как операторы программ-вымогателей атаковали российский бизнес в 2021» ноябрь 2021 URL: https://www.group-ib.ru/whitepapers/ransomware-in-russia-2021.html

9. [Электронный ресурс] Информационный веб-сайт компании Kaspersky URL: https://www.kaspersky.ru/blog/ (Дата обращения: 12.03.2022)

10. [Электронный ресурс] Информационный сайт компании Verizon Business, предоставляющие передовые информационные технологии URL: https://www.verizon.com/business/ (Дата обращения: 14.03.2022)

11. [Электронный ресурс] // Информационный портал по безопасности SecurutyLab

12. URL: https://www.securitylab.ru/ (Дата обращения: 12.03.2022)

13. [Электронный ресурс] Информационный сайт Федеральной службы государственной статистики. Федеральный закон от 27.07.2006 № 149-ФЗ URL: https://rosstat.gov.ru/storage/mediabank/Федеральный%20закон%20от%2027.07.2006%20№149-ФЗ_ред%2001-12-2021.pdf (Дата обращения:12.06.2022)

14. [Электронный ресурс] Официальный сайт ФСТЭК России. Письмо ФСТЭК России от 20 марта 2020 г. N 240/84/389 URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2059-pismo-fstek-rossii-ot-20-marta-2020-g-n-240-84-389 (Дата обращения: 13.06.2022)

## INFORMATION SECURITY IN THE CONDITIONS OF REMOTE WORK OF EMPLOYEES

***M.O. Pyankov, E.Yu. Nikitina***

Perm State National Research University

**Abstract.** This article discusses such questions as: the relevance of information security in the conditions of remote work of employees, factors of increasing vulnerability when working from home, the goals of malicious intruders and the tools with which they gain unauthorized access. What specific actions of employees lead to the loss of information, as well as the number of ransoms paid by companies that have become victims of intruders.

**Keywords:** *security, access, remote work, malicious, loss of information.*

# ОСОБЕННОСТИ ПОДГОТОВКИ КАДРОВ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

***А.В. Шабурова, А.В. Троеглазова, Т.А. Самойлюк***
Сибирский государственный университет геосистем и технологий

**Аннотация.** В работе приводятся результаты анализа основных характеристик образовательных программ по направлениям подготовки 10.03.01 Информационная безопасность, 12.03.01 Приборостроение, 12.03.02 Оптотехника, 12.03.03 Фотоника и оптоинформатика, 27.03.01 Стандартизация и метрология, 27.03.05 Инноватика и 17.05.01 Боеприпасы и взрыватели на предмет наличия в них цифровых компетенций и дисциплин, позволяющих осуществлять формирование цифровых навыков. Представленные в ФГОС ВО 3++ общепрофессиональные цифровые компетенции недостаточны для формирования цифровых навыков у выпускников инженерных направлений подготовки, поэтому формирование навыков программной инженерии осуществляется при изучении профильных дисциплин. Составлен перечень дисциплин, позволяющих сформировать навыки цифровой грамотности, алгоритмического мышления и применения языков программирования, применения методов искусственного интеллекта. Оценка степени сформированности цифровых компетенций проведена путем анкетирования студентов 2–4 курсов перечисленных направлений подготовки.
**Ключевые слова:** *цифровые компетенции, информационная безопасность, уровень сформированности*

В реалиях настоящего времени значимость освоения цифровых навыков не вызывает сомнений не только при подготовке специалистов в области информационных технологий, но и инженерных направлений подготовки. К цифровым компетенциям можно отнести не только цифровую грамотность, но и медиа- и коммуникативную грамотность, навыки программирования, навыки применения методов искусственного интеллекта и т.д. [1–3].

В институте оптики и технологий информационной безопасности (ИОиТИБ) Сибирского государственного университета геосистем и технологий подготовка студентов осуществляется по шести направлениям и одной специальности, перечень которых с указанием профиля подготовки представлен в таблице 1.

*Таблица 1*

*Перечень направлений подготовки ИОиТИБ*

| Шифр направления подготовки | Наименование направления подготовки | Профиль |
|---|---|---|
| 10.03.01 | Информационная безопасность | Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности) |
| 12.03.01 | Приборостроение | Технология приборостроения |
| 12.03.02 | Оптотехника | Оптико-электронные приборы и системы |
| 12.03.03 | Фотоника и оптоинформатика | Приборы квантовой электроники |
| 27.03.01 | Стандартизация и метрология | Стандартизация и метрология |
| 27.03.05 | Инноватика | Управление инновациями |
| 17.05.01 | Боеприпасы и взрыватели | Взрыватели |

Цель настоящей работы заключалась в выявлении особенностей подготовки кадров инженерной направленности при реализации цифровых компетенций. Для достижения поставленной цели были решены следующие задачи:

– проведен анализ общих характеристик основных образовательных программ по выявлению перечня цифровых компетенций при их сопоставлении с изучаемыми дисциплинами;

– проведена оценка уровня сформированности цифровых компетенций у студентов 2–4 курсов перечисленных направлений подготовки и специальности (табл. 1).

Осваиваемые студентами цифровые компетенции классифицировали по трем группам. Первая группа компетенций «Цифровая грамотность» предполагает формирование навыков сбора, представления, хранения и обработки информации всеми доступными способами; знание основ информационной безопасности и формирование базовых навыков защиты информации; формирование навыков установки стандартного программного обеспечения, подключения и применения стандартного периферийного оборудования.

К компетенциям второй группы «Алгоритмическое мышление и программирование» относятся применение языков программирования, алгоритмов структуры данных, основ программной инженерии, разработка веб-приложений и т.д.

Третья группа компетенций «Анализ данных и методы искусственного интеллекта» позволяет сформировать у обучающихся навыки машинного обучения, обработки и интеллектуального анализа данных и пр.

Дисциплины, изучаемые студентов перечисленных направлений подготовки, распределены между тремя группами цифровых компетенций (табл. 2).

*Таблица 2*

*Перечень направлений подготовки ИОиТИБ*

| Шифр направления поготовки | Группа компетенций | | |
|---|---|---|---|
| | Группа 1 | Группа 2 | Группа 3 |
| *12.03.01* | Информатика; компьютерная и инженерная графика; основы информационной безопасности | Компьютерные технологии в приборостроении; промышленные робототехнические системы | Системы искусственного интеллекта |
| *12.03.02* | Информатика; компьютерная и инженерная графика; основы информационной безопасности в оптотехнике | Основы проектирования и конструирования | Системы искусственного интеллекта |

*Окончание табл. 2*

| Шифр направления поготовки | Группа компетенций | | |
|---|---|---|---|
| | Группа 1 | Группа 2 | Группа 3 |
| *12.03.03* | Информатика; компьютерная и инженерная графика; основы информационной безопасности; теория информации и информационных систем; введение в квантовую информатику | Основы проектирования и конструирования; основы оптоинформатики; технологии программирования | Системы искусственного интеллекта; технологии искусственного интеллекта |
| *27.03.01* | Информатика; компьютерная и инженерная графика | Промышленные робототехнические системы; 3D-прототипирование | Системы искусственного интеллекта |
| *27.03.05* | Информатика; основы управления информационной безопасностью; защита информации | Методы и средства проектирования информационных систем и технологий; алгоритмы решения нестандартных задач | Системы искусственного интеллекта |
| *17.05.01* | Информатика; компьютерная и инженерная графика; основы управления информационной безопасностью | Информационные компьютерные среды проектирования и сопровождения жизненного цикла боеприпасов и взрывателей | Системы искусственного интеллекта |
| *10.03.01* | Информатика; основы информационной безопасности; информационно-аналитическая деятельность по обеспечению комплексной безопасности; управленческая деятельность в сфере информационной безопасности; организационное и правовое обеспечение информационной безопасности; основы управления информационной безопасностью; защищенные автоматизированные системы; методы и средства криптографической защиты информации; сети и системы передачи информации; защита информации от утечки по техническим каналам | Компьютерная и инженерная графика; основы автоматизированного конструирования средств защиты информации; языки программирования; технологии и методы программирования; встраиваемые системы и их программирование; программно-аппаратные средства защиты информации; системы обнаружения вторжений | Системы искусственного интеллекта; технологии и методы искусственного интеллекта |

Оценку уровня сформированности цифровых компетенций проводили путем анализа результатов анкетирования студентов по двум группам: 1 группа – цифровая грамотность и 2 группа – алгоритмическое мышление и программирование. Полученные результаты представлены на рисунках 1 и 2.

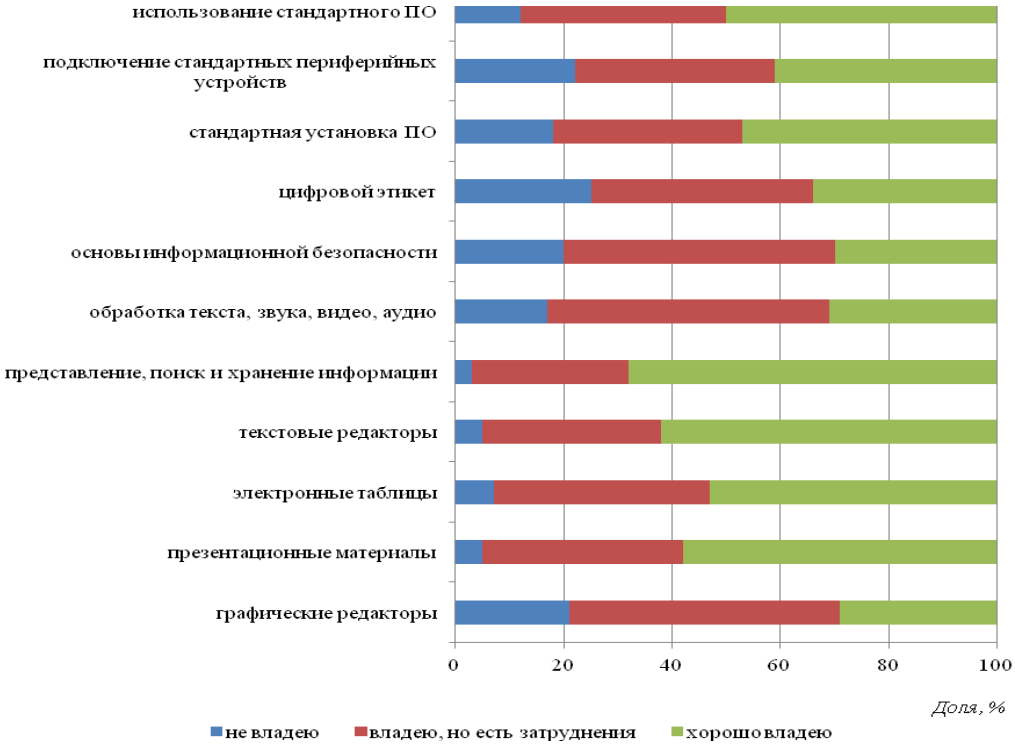



*Рис. 1. Результаты оценки уровня владения компетенциями «Цифровая грамотность»*

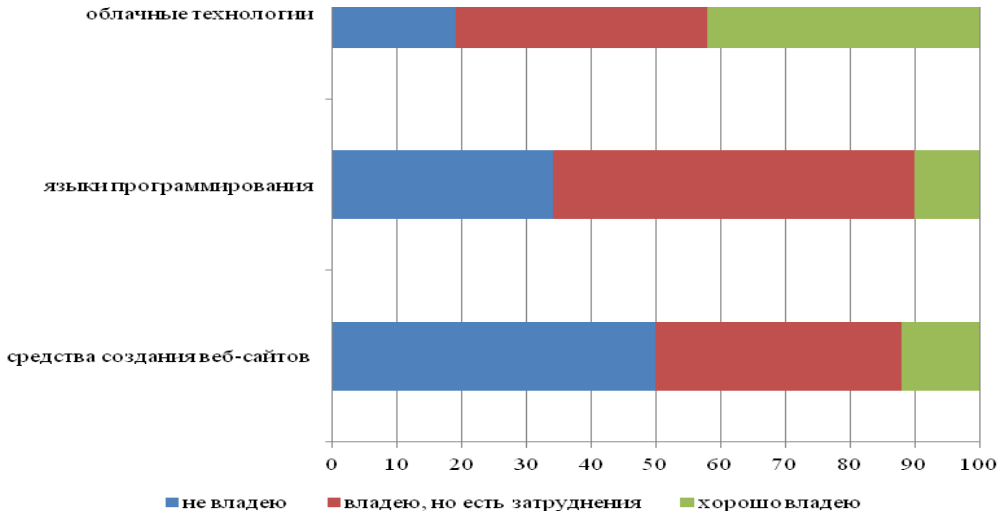



*Рис. 2. Результаты оценки уровня владения компетенциями «Алгоритмическое мышление и программирование»*

Для повышения уровня сформированности цифровых компетенций необходимо выполнений нескольких условий:

– обеспечение последовательности и комплексности формирования цифровых компетенций при изучении всего цикла дисциплин;

– наличие развитой материально-технической базы;

– профессиональный профессорско-преподавательских состав, обладающий высоким уровнем цифровых компетенций;

– использование в образовательном процессе эффективных технологий обучения, в том числе проектного обучения.

## Список литературы

1. Дмитриев Я.В., Алябин И.А., Бровко Е.И., Двинина С.Ю., Демьянова О.В. Развитие цифровых навыков у студентов вузов: де-юре vs де-факто // Университетское управление: практика и анализ. – 2021. 25(2). С. 59–79.

2. Пеша А.В. Развитие надпрофессиональных компетенций студентов в формате онлайн // Мир науки. Педагогика и психология. 2020. № 3. Т. 8. С. 1–17.

3. Ломаско П.С. Методические особенности подготвоки кадров в области современных информационных технологий в условиях становления смарт-образования // Мир науки. 2017. № 6. Т. 5. С. 1–12.

## PECULIARITIES OF PERSONNEL TRAINING IN THE CONTEXT OF THE DEVELOPMENT OF THE INFORMATION SOCIETY

***A.V. Shaburova, A.V. Troeglazova, T.A. Samoylyuk***
Siberian State University of Geosystems and Technologies

**Abstract.** The paper presents the results of the analysis of the main characteristics of educational programs in the areas of training 10.03.01 Information security, 12.03.01 Instrumentation, 12.03.02 Optotechnics, 12.03.03 Photonics and optoinformatics, 03.27.01 Standardization and metrology, 03.27.05 Innovation and 17.05 .01 Ammunition and fuses for the presence of digital competencies and disciplines that allow the formation of digital skills. The general professional digital competencies presented in the FSES HE 3++ are not sufficient for the formation of digital skills among graduates of engineering areas of training, therefore, the formation of software engineering skills is carried out in the study of specialized disciplines. A list of disciplines has been compiled that allows you to form the skills of digital literacy, algorithmic thinking and the use of programming languages, the use of artificial intelligence methods. The assessment of the degree of formation of digital competencies was carried out by questioning students of 2-4 courses of the listed areas of training.

**Keywords:** *digital competencies, information security, level of maturity.*

# КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

***Н.А. Шардаков, М.Ю. Карпов***
Пермский государственный национальный исследовательский университет

**Аннотация**. В рамках исследовательской работы по теме «Конфиденциальность персональных данных» доказывается актуальность проблемы конфиденциальности персональных данных. Основная проблематика данной статьи: нарушение конфиденциальности данных. Цель данной статьи – выяснить, что является персональными данными, какими средствами поддерживается конфиденциальность персональных данных, основные причины утечки данных, способы защиты. Задачи данной статьи – рассмотреть основные причины утечки персональных данных и их последствия, предложить вариант решения данной проблемы. В качестве доказательства актуальности проблемы, представлены результаты опроса, цель которого выявить уровень осведомленности граждан в сфере персональных данных.
**Ключевые слова**: *персональные данные, конфиденциальность, защита, утечка, информация, последствия, причины, законодательство*.

## Введение

Повседневная жизнь современного человека напрямую связана с Интернетом и его возможностями во всех сферах жизни. Ежедневно человек предоставляет свои персональные данные различным организациям и ресурсам (банки, социальные сети, медийные сервисы, различные компании и т.д.). Все эти организации и ресурсы для правильной работы и улучшения продаваемых услуг требуют внести персональные данные пользователя. Например, при выпуске банковской карты, банк у своего клиента обязательно запросит паспортные данные, дату рождения, фамилию, имя, отчество. Без этих данных корректная работа банковского счета и совершение денежных транзакций невозможна.

Для защиты своих данных от третьих лиц пользователи используют различные пароли, шифры, ключи и т.д. В свою очередь организации и ресурсы предоставляют пользователям политику конфиденциальности, а государство создаёт правовую основу для регулирования персональных данных. Пренебрегая надежной защитой персональных данных, пользователи становятся жертвами мошенников (шантаж, угрозы, неправомерное использование данных, вмешательства в личную жизнь, разглашение личной информации).

## Актуальность проблемы

Проблема конфиденциальности персональных данных очень актуальна в наше время. Люди не знают и не понимают, кому и с какой целью предоставляют свои данные и как правильно обеспечить их защиту.

В доказательство актуальности данной проблемы хочу привести результаты собственного исследования (анализ собственного исследования приведен

в отдельном пункте) и исследования крупных компаний. Исследование Pew Research Center (исследовательский центр, собирает информацию о социологических проблемах, формирующихся в США и мире) показывает, что 79% американских респондентов знаю о том, что крупные компании собирают персональные данные в Интернете и используют их для рассылки рекламы и составления портрета потребителя. 13% американских респондентов утверждают, что всегда читают политику конфиденциальности. Результаты исследования Cisco Privacy Survey (Cisco – крупная организация по продаже сетевого оборудования) показывают, что 45% респондентов обвиняют государство в том, что оно оперирует персональными данными в собственных целях. По информации ООН 18% развитых стран не имеет законодательства по регулированию персональных данных [5].

## Персональные данные

Для обеспечения конфиденциальности персональных данных необходимо понимать, что к ним относится и в какой форме они представлены.

*Персональные данные* – любая информация, относящаяся прямо или косвенно определенному физическому лицу. Примеры персональных данных: фамилия, имя, отчество, дата рождения, фотография или видеозапись человека, местожительства, семейное положение, информация о состоянии здоровья, образование, уровень дохода, раса, религия и так далее. Стоит учитывать, что некоторые данные попадают под категорию «персональных» только в связке с другими данными. Например: просто номер телефона не является персональными данными, но если к этому номеру приписать ФИО владельца, то такие данные уже относятся к «персональным».

*Конфиденциальность информации* – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать информацию третьим лицам без согласия ее обладателя.

*Хранение персональных данных* – сохранение данных на каком-либо носителе информации.

*Обработка персональных данных* – любые действия над данными, в том числе сбор, анализ, изменение и удаление [4].

Согласно совместному приказу ФСТЭК, ФСБ и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 года «Об утверждении Порядка проведения классификации информационных систем персональных данных» персональные данные разделяются на несколько классов:

- Класс 1: персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.
- Класс 2: персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нём дополнительную информацию.
- Класс 3: персональные данные, позволяющие идентифицировать субъекта персональных данных.
- Класс 4: обезличенные или общедоступные персональные данные [8].

Также данные разделяют на общие, специальные, биометрические и иные. *Общими* являются те данные, на которые дано согласие субъекта данных. На такие данные не распространяется закон о соблюдении конфиденциальности. Яркий пример таких данных – это информация, которая содержится в профилях в социальных сетях или на сайтах объявлений. К *специальным* данным относится информация о расе, национальности, религии, политических и философских взглядах, здоровье, судимостях. Такие данные уже трудно найти в открытом доступе. Их можно узнать только лично у субъекта данных или у оператора, который обрабатывает эти данные. Субъект имеет право не разглашать эти данные. *Биометрические данные* – физиологические или биологические особенности человека, с помощью которых можно установить личность. Например: отпечаток пальца, радужная оболочка глаза, форма лица, голос, фотография, группа крови. Биометрические данные могут обрабатываться только при наличии согласия в письменной форме. Обработка биометрии без согласия может осуществляться в случаях, предусмотренные законодательством Российской Федерации (правосудие, оперативно-розыскная деятельность, выезд и въезд на территорию РФ) [4]. В последнее время набирает популярность авторизации (или подтверждение личности) с помощью биометрии. Почти в каждом современном смартфоне для разблокировки устройства, получения доступа к защищенным данным, подтверждения бесконтактных платежей используется отпечаток пальца или скан формы лица владельца этого устройства. Некоторые банки для подтверждения личности уже используют биометрические данные клиентов. Например, российский банк «СберБанк» в своих офисах с помощью распознавания лица может идентифицировать клиента без дополнительных документов. При звонке в контактный центр для установления личности клиента используется голосовая биометрия. Банкоматы этого банка уже поддерживают функцию «Оплата одним взглядом». Также в России создана единая биометрическая система – цифровая платформа, которая позволяет гражданину проходить удалённую идентификацию по биометрии для получения государственных услуг. *Иные персональные данные* – это все данные, которые не относятся к

общедоступным, специальным, биометрическим. Например: принадлежность к определённой социальной группе, уровень дохода, стаж работы. Иные данные очень подходят по описание «специальных», но такие данные зачастую никак не характеризуют человека (дополнительная информация о человеке) и могут часто меняться [4].

**Законодательство по регулированию персональных данных**

Как было сказано выше, человек ежедневно предоставляет доступ к своим персональным данным. Развитие технологий даёт возможность обрабатывать, собирать и распространять данные автоматически. Зачастую человек не может самостоятельно противодействовать посягательству на его частную жизнь. Государство для обеспечения безопасности своих граждан создаёт правовые акты по регулированию персональных данных, защите прав человека и по предотвращению незаконного сбыта этих данных.

Персональные данные попадают под «Перечень сведений конфиденциального характера», утвержденный Указом Президента Российской Федерации от 13 июля 2015 г.

По характеру содержания, информация делится на государственную тайну и конфиденциальную информацию. Государственная тайна имеет несколько грифов секретности: «особой важности», «совершенно секретно», «секретно».

К конфиденциальной информации относят сведения, составляющие:

1. Коммерческая тайна.
2. Служебная тайна.
3. Профессиональные тайны.
4. Персональные данные [7].

Основным документом по регулированию персональных данных на территории Российской федерации является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Цель данного закона – обеспечить защиту прав и свобод гражданина при обработке его персональных данных. В этом документе прописаны основные понятия, связанные с обработкой данных, принципы осуществления обработки информации ограниченного доступа, обязанности оператора, права субъекта персональных данных, виды ответственности за нарушение требований. Также данный закон регулирует отношения, связанные с обработкой персональных данных, между субъектом и оператором.

Основные принципы обработки персональных данных на территории РФ:

1. Обработка персональных данных только на законной основе.
2. Обработка персональных данных должна ограничиваться достижением конкретной цели.

3. Обработке подлежать только те данные, которые отвечают целям их обработки.

4. Оператор должен принимать необходимые меры по уточнению актуальности данных и по удалению неполных или неточных данных.

5. Оператор персональных данных обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

6. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические данные), могут обрабатываться только при наличии согласия в письменной форме.

7. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных.

8. Трансграничная передача данных на территории иностранных государств возможна только с обеспечением адекватной защиты прав субъекта персональных данных.

В случае нарушения законодательства при обработке данных оператор обязан:

1. Заблокировать неправомерно обрабатываемую информацию.

2. Прекратить обработку персональных данных.

3. Уведомить субъекта данных о допущенных нарушениях при обработке данных.

4. Уничтожить персональные данные.

Проверкой по соблюдению и реализации законов (регуляторы) в области защиты персональных данных занимаются следующие государственные органы:

1. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

2. Федеральная служба по техническому и экспортному контролю.

3. Федеральная служба безопасности Российской Федерации [6].

Правовое регулирование персональных данных на территории государства является первым шагом для обеспечения защиты, конфиденциальности и сохранности персональных данных и неприкосновенности личной жизни граждан.

## Политика конфиденциальности

Политика конфиденциальности (Privacy Policy) – это документ, в котором раскрываются некоторые или все способы, с помощью которых сайт собирает, использует и раскрывает персональные данные посетителей сайта.

Обычно политика конфиденциальности включает в себя:

1. Наименование компании, адрес, контактные данные.
2. Определения терминов.
3. Общие положения.
4. Предмет политики конфиденциальности.
5. Цели сбора персональной информации.
6. Способы и сроки обработки персональной информации.
7. Обязательства и ответственность сторон [3].

Согласно законодательству России оператор персональных данных должен предупредить субъекта о сборе персональных данных и взять согласие на обработку данных. Именно политика конфиденциальности определяет, что относится к персональным данным, как оператор их собирает, обрабатывает, хранит и кому передаёт.

Политику конфиденциальности должны публиковать на своём ресурсе все операторы, которые обрабатывают персональные данные. Если на сайте есть разделы «Регистрация», «Обратная связь», «Оформить заказ», «Купить», «Доставка» и так далее, то обязательно у ресурса должна быть политика конфиденциальности. Чтобы не пугать своих потенциальных клиентов «страшными» словами и законами, зачастую раздел с политикой конфиденциальности располагается в самом низу сайта или приложения. Закон не определяет, где именно должен находиться текст политики конфиденциальности. Главное, чтобы у пользователей был свободный доступ к тексту политики.

При переходе на какой-либо ресурс, может появиться всплывающее окно «Сайт использует файлы cookie, что позволяет получать информацию о вас. Продолжая пользоваться сайтом, вы соглашаетесь с политикой конфиденциальности». Файлы cookie (находятся в рабочих файлах самого браузера) собирают информацию о посещенных страницах и времени, проведённом на сайте, а также фиксируют отдельные действия на сайте. Cookie файлы также собирают информацию о версии браузера, операционной системы, типа устройства. Злоумышленники могут перехватить содержание cookie файлов через незашифрованное соединение и извлечь конфиденциальную информацию (в дальнейшем использовать эту информацию против её обладателя). Чтобы предотвратить кражу cookie файлов необходимо использовать только защищенное соединение HTTPS, не совершать каких-либо банковский транзакций или авторизаций через общественные точки доступа в Интернет, не пользоваться сомнительными ресурсами [3].

Главная проблема – люди не читают политику конфиденциальности и просто так принимают условия, ставя галочку «Я принимаю условия» (поставить галочку легче, чем прочитать 3–4 страницы юридического текста). Пользователь не знает, какие личные данные собираются, куда отправляются и как

используются. Такое «не знание» может привести к нарушению конфиденциальности персональных данных. В качестве примера хочу привести ресурс LightShot. *LightShot* – программа для захвата экрана и дальнейшего редактирования. Программа даёт возможность легко сделать скриншот нужной области экрана и поделиться этим скриншотом с другими людьми. После захвата нужной части экрана, скриншот отправляется на сервер и пользователю предоставляется короткая, удобная ссылка на этот скриншот. На все скриншоты идёт один тип ссылки: https://prnt.sc/******, где ***** произвольная комбинация из цифр и английских букв установленной длины (5–6 знаков). Злоумышленник, не прилагая особых усилий, может легко автоматизировать процесс сбора скриншотов по ссылкам и украсть персональные данные пользователей. В свою очередь пользователи, не прочитавшие политику конфиденциальности, начинают сами, добровольно выкладывать свои данные. Среди таких данных: скриншоты паспортов, логинов, паролей, документов, банковских чеков и транзакций и так далее. Такие пользователи считают, что скриншоты хорошо защищены и доступ будет только у того, кому была отправлена ссылка на скриншот. Сам сервис этого не скрывает и прямо объясняет это в своей политики конфиденциальности:

«*В частности, каждое изображение, загруженное (даже если оно было загружено в вашу галерею) на этот веб–сайт, является общедоступным – независимо от того, загружено ли оно напрямую без входа в учетную запись пользователя или загружено через учетную запись пользователя – и имеет свой собственный URL-адрес. К каждому изображению всегда может получить доступ и просмотреть любой, кто введет именно этот URL-адрес. Ни одно изображение, загруженное на этот веб-сайт, никогда не бывает полностью скрыто от всеобщего обозрения. Это делается для того, чтобы гарантировать, что этот веб-сайт не будет использоваться в качестве платформы для незаконных действий. Функциональность нашего веб-сайта не предназначена для того, чтобы быть безопасной платформой; она предназначена для обмена изображениями*.»

Перед использованием ресурса важно прочесть политику конфиденциальности. Прочитав её, Вы на 50% обезопасите свои персональные данные и будете знать, где и как они используются, и куда нужно обратиться, чтобы персональные данные удалили с ресурса [12].

## Информационная система персональных данных

*Информационная система персональных данных (ИСПДн)* – информационная система, представляющая собой совокупность персональных данных, которые хранятся в базах данных, позволяющих проводить обработку персональных данных с помощью средств автоматизации (или без автоматизации). Информационные системы персональных данных помогают различным организациям обрабатывать персональные данные субъектов, в том числе – автоматизированная обработка [4].

Согласно приказу ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 18.02.2009 г. «Об утверждении порядка проведения классификации информационных систем персональных данных» информационные системы делятся на 2 класса:

- *1 класс:* Типовые информационные системы – системы, где требуется обеспечить только конфиденциальность обрабатываемых персональных данных.
- *2 класс:* Специальные информационные системы – системы, где требуется обеспечить одну из характеристик безопасности отличную от конфиденциальности (например, целостность или доступность).

Также информационные системы разделяются на категории в зависимости от количества субъектов:

- *1 категория:* в информационной системе одновременно обрабатываются персональные данные более чем 100.000 субъектов.
- *2 категория:* в информационной системе одновременно обрабатываются персональные данные от 1.000 до 100.000 субъектов.
- *3 категория:* в информационной системе одновременно обрабатываются персональные данные менее 1.000 субъектов [8].

Информационные системы персональных данных, также как и другая информация, подвержены угрозам несанкционированного доступа. Такие системы наиболее уязвимы, из-за больших объемов обрабатываемой информации, сосредоточение в базах данных информации разной важности и конфиденциальности, расширенный доступ круга пользователей, увеличенное число удалённых рабочих мест, повсеместное использование различных каналов связи (в том числе сеть Internet), автоматизация обработки данных.

Причины несанкционированного доступа к информации – это слабая защита или её отсутствие.

Технические каналы утечки информации:

- *Акустические каналы:* специальные устройства негласного съёма информации (например, диктофон, радиомикрофоны и т.п.).

- *Электромагнитные и проводные каналы:* побочные электромагнитные излучения и наводки.
- *Оптический (видовой) канал:* визуальное наблюдение и съемка носителей (фото-, видеосъемка).

Применение высокотехнологичных устройств, при использовании технического канала, должны быть оправданы ценностью информации.

Помимо технических каналов, угрозой нарушения конфиденциальности могут стать физические лица. Такие лица делятся на 2 типа:

- *Внешние нарушители* – нарушители, не имеющие права доступа к информационной системе, реализующие угрозы из внешних сетей общего пользования. Внешними нарушителями могут быть: разведывательные службы иностранных государств, криминальные структуры, конкуренты, недобросовестные партнеры, политические противники.
- *Внутренние нарушители* – нарушители, имеющие право постоянного или разового доступа к информационной системе, реализующие угрозы непосредственно в информационной системе. Возможности внутреннего нарушителя зависят от действующей защиты информационной системы, в том числе порядок доступа физических лиц к информационной системе. Внутренними нарушителями могут быть: персонал учреждения, персонал филиалов, лица с нарушенной психикой, специальные агенты.

Такие нарушители, а если точнее их действия, могут привести к следующим последствиям:

- Кража (ноутбуки, жесткие диски, ключи доступа, носители информации)
- Подмена (операционные системы, СУБД, прикладное ПО, пароли)
- Уничтожение (носители информации, данные, пароли, аппаратура)
- Нарушение нормальной работы (скорость обработки информации, нарушение пропускной способности каналов, нарушение электроснабжения)
- Ошибки (настройка оборудования, прикладное ПО)

Возможные объекты атак:

- Документация на криптосредство и на технические и программные компоненты
- Защищаемые персональные данные
- Аутентифицирующая и парольная информация
- Криптографически опасная информация
- Данные, передаваемые по каналам связи
- Помещения, в которых находятся защищаемые ресурсы информационной системы [1]

Каждая реализованная угроза (нарушение) повлечет за собой убытки: раскрытие защищаемой информации, нарушение работы информационной системы, оборот ложной информации, урон деловой репутации, ошибочные решения. А иногда повлечет и непосредственную угрозу жизни.

Оценка опасности угроз:

- *Низкая опасность* – незначительные негативные последствия для субъектов персональных данных (аппаратные закладки, ПО, не связанное с работой ИС, электромагнитные излучения и т.д.)
- *Средняя опасность* – негативные последствия для субъектов персональных данных (кража ключей доступа, стихийное бедствие, сбой электроснабжения, файловый вирус и т.д.)
- *Высокая опасность* – значительные негативные последствия для субъектов персональных данных (утрата ключей и атрибутов доступа)

Для обеспечения безопасности данных, хранящиеся в информационной системе, каждая информационная система должна иметь разработанную «Частную модель актуальных угроз». В данном документе перечислены самые потенциальные угрозы из всех возможных [4].

Согласно приказу ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» каждая информационная система должна пройти аттестацию. Для частных информационных систем аттестация добровольная, для государственных – обязательная. Аттестация проводится учреждением/организацией, обладающей лицензией на ведение дел по технической защите информационных ресурсов. В случае выявления недостатков в процессе аттестации, работы приостанавливаются до устранения этих недостатков [9].

Согласно приказу ФСТЭК от 18.02.2013 № 32 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» в каждую информационную систему должны входить следующие меры по обеспечению безопасности персональных данных:

- Идентификация и аутентификация субъектов и объектов доступа
- Ограничение программной среды
- Защита носителей персональных данных
- Регистрация событий безопасности
- Антивирусная защита
- Обнаружение и предотвращение вторжений
- Контроль защищенности персональных данных

- Защита технических средств
- Защита информационной системы, её средств, систем связи и передачи данных [10]

Для защиты персональных данных в информационной системе мероприятия по защите этих данных должны проводиться для всех возможных видов угроз. Также необходимо обращать особое внимание на нейтрализацию актуальных угроз.

**Причины нарушения конфиденциальности персональных данных**

*Угроза безопасности персональных данных* – условия и факторы, создающие опасность несанкционированного (случайного) доступа к персональным данным.

Существует множество способов нарушения конфиденциальности персональных данных: от человеческого фактора до технических аспектов.

В современных организациях работники во время исполнения своих обязанностей (например, при обработке персональных данных) могут нарушить конфиденциальность информации: случайно или умышленно. Зачастую, злоумышленники подкупают сотрудника организации, и он даёт доступ к данным клиентов или другой конфиденциальной информации. 66 % случаев утечек данных в 2018 году произошло по вине сотрудников организаций.

Также одной из причин утечки и нарушения конфиденциальности информации является плохая защита баз данных, информационных систем. Ненадежная, слабая защита с множеством ошибок не может отразить атаки злоумышленников. Злоумышленники взламывают системы, получают полный доступ к конфиденциальной информации и начинают использовать её в незаконных целях.

Ещё одна из причин утечки данных – это фишинговые рассылки. *Фишинг* – способ получения конфиденциальной информации, основанный на незнании пользователями основ сетевой безопасности. Задача таких рассылок – обмануть, запутать жертву и заставить перейти по вредоносной ссылке, отправить свои данные через поддельную форму. Чтобы «втереться» в доверие жертвы, мошенники незначительно меняют доменный адрес почтового сервера или название организации (например, правдивый адрес @psu.ru, мошенники могут использовать psn.ru, или google.com – qoogle.com). Также такие сообщения обычно безличные, так как рассылки производятся массово и правдивые имена жертв неизвестны (например, «Дорогой клиент! «, «Уважаемый сотрудник! «).

Простой поиск информации в открытых источниках (*интернет-парсинг*) – тоже является одной из причин нарушения конфиденциальности информации. Пользователи сами оставляют о себе много данных, большая часть из этих дан-

ных является лишней (например, ссылки на свои аккаунты на других сервисах, которые содержат другую, более подробную конфиденциальную информацию). Анализ социальных сетей, личных страничек жертвы, форумов не затратит у мошенника много времени. За 2–3 часа злоумышленник может узнать интересы жертвы, место работы, имена родственников и так далее. С помощью этой информации мошенник может «подогнать» фишинговое письмо, чтобы оно стало еще более достоверным, или использовать в других незаконных целях [12].

Вредоносная программа также является одной из причин нарушения конфиденциальности. Неопытный пользователь может не заметить на своем рабочем месте вредоносную программу, которая без ведома пользователя «выкачивает» его персональные данные. Такая вредоносная программа может быть специально установлена злоумышленником, либо из-за незнаний пользователь сам установил эту программу (например, через фишинговое письмо).

Мошенник также банально может подсмотреть, подслушать или перехватить конфиденциальную информацию. Для подсматривания информации могут быть использованы различные оптические средства или видеозакладки. Речевую информацию мошенник может подслушать через технические каналы или с помощью различной акустической аппаратуры. Перехват информации реализуется «прослушиванием сети». *Sniffer* – специальная программа-анализатор, которая перехватывает все пакеты, которые идут по сети. Таким способом очень часто «ловят» пароли и идентификаторы пользователя.

**Последствия от нарушения конфиденциальности персональных данных**

Важно понимать, к каким последствиям может привести утечка персональных данных. Последствия могут оказаться серьезными так для жертвы, так и для злоумышленника.

В первую очередь от утечки персональных данных пострадает жертва. Личная информация может стать общедоступной. Злоумышленник может угрожать жертве или шантажировать её (вымогательство денег, месть личного характера, принуждение к каким-либо действиям, насилие). От утечки данных могут пострадать и банковские счета – неправомерное списание средств. С помощью «слитых» данных, мошенник может вмешиваться в личную жизнь жертвы. Злоумышленник может «прикрываться» Вашими данными при совершении другого противоправного деяния. Самое безобидное, что может произойти при утечке данных – это рассылка рекламных объявлений или спам (утечка адреса электронной почты, номера телефона) [13].

От утечки персональных данных также пострадают и злоумышленники. Они могут понести гражданскую (взыскание убытков), административную (наложение штрафа, приостановления или запрет конкретной деятельности)

или уголовную ответственность. На сегодняшний день, иски, связанные с нарушением конфиденциальности персональных данных, серьёзно не рассматриваются. Даже если суд и установил неправомерное действие над персональными данными, то размер штрафа редко превысит десять тысяч рублей. Наказание будет серьёзнее, если в ситуацию вмешаются регуляторы в области персональных данных (Роскомнадзор, ФСТЭК, ФСБ) – возбуждение уголовного дела [5].

**Способы защиты, сохранения конфиденциальности персональных данных**

Для обеспечения сохранности персональных данных, необходимо, чтобы меры по защите информации выполняли как операторы персональных данные, так и владельцы этих данных. Рассмотрим меры защиты для операторов и субъектов по отдельности.

В первую очередь, операторы персональных данных должны соблюдать требования законов, указов, постановлений в данной области. Для устранения внутренних нарушителей (сотрудники организации) необходимо обучать персонал, объяснять им все аспекты работы с конфиденциальной информацией. Также необходимо установить уровни доступа сотрудников к конфиденциальной информации и фиксировать все действия сотрудников над этой информацией. Технические средства по обработке, хранению и передаче персональных данных должны быть хорошо защищены от атак: установка межсетевых экранов (Firewall, фильтрация сетевого трафика), установка антивирусных программ, использование современного оборудования. Использовать методы криптографической защиты при шифровании данных. Для обеспечения защиты корпоративных сетей необходимо использовать DLP (Data Leak Prevention) системы. DLP система анализирует потоки входных и выходных данных защищаемой системы, при обнаружении запрещённой информации – поток блокируется. DLP система, например, может оградить сотрудников организации от фишинговых писем [2].

Субъекты персональных данных должны проявлять бдительность при использовании своих данных и обеспечивать защиту этих данных различными методами.

Рассмотрим основные правила при работе с персональными данными:

- Не стоит передавать свои данные сомнительным организациям (в том числе организациям, которые не зарегистрированы как оператор персональных данных).
- Проводить интернет-платежи только на официальных, правдивых сервисах.
- Уточнять достоверность информации.

- Изучать политику конфиденциальности. Понимать цель обработки персональных данных.
- Указывать только необходимый минимум персональных данных.
- Использовать только защищённое соединение. [12]

Рассмотрим самые распространённые способы защиты данных:

- Парольная аутентификация. *Пароль* – произвольный набор символов, который предназначен для подтверждения личности или полномочий. Необходимо использовать разные пароли достаточной сложности на разных сервисах, регулярно обновлять пароли. Не рекомендуется использовать легкие пароли: дата рождения, имя, номер телефона, password, qwerty123 и так далее. Надежный пароль должен содержать не менее 8-10 символов с использованием цифр, различных знаков и символов разных регистров (Например, Fg4m67A#5). Не стоит хранить пароли на других носителях информации: листочки, блокноты, записи в паспорте, заметки на смартфоне, в личных сообщениях социальной сети или мессенджера.
- Двухфакторная аутентификация. *Двухфакторная аутентификация* – это идентификация пользователя при помощи запроса аутентификационных данных двух разных тип. Обычно на практике это пароль и какой-либо одноразовый код (приходит по SMS или электронной почте), реже USB-ключ и биометрические данные. Двухфакторная аутентификация серьёзно усложняет злоумышленникам доступ к конфиденциальной информации. В случае если злоумышленник сможет украсть или подобрать пароль, то для доступа к данным ему еще необходимо получить одноразовый код, который придет владельцу данных на телефон или электронную почту. На сегодняшний день почти все социальные сети, мессенджеры, интернет-банкинг и другие сервисы поддерживаю возможность подключения двухфакторной аутентификации. Прохождение двухфакторной аутентификации довольно долгая и неприятная процедура, поэтому необходимо устанавливать этот метод защиты на тех ресурсах, где содержатся важные для вас данные (соц. сети, мессенджеры, банки, почта) [2].
- Менеджеры паролей. *Менеджер паролей* – это специальная программа, которая хранит пароли, логины, PIN-коды, данные банковских карт в зашифрованном виде и служит для облегчения авторизации на сайтах или в приложениях. Неопытные или ленивые пользователи, чтобы не запоминать сложную и длинную последовательность символов, в качестве паролей ставят qwerty123, password, admin, тем самым подвергают опасности свои данные. Менеджер за вас запомнит сложные пароли и автоматически использует их по вашему запросу. Большинство пользователей знают о таких сервисах, но не пользуются ими – боятся, что их пароли украдут. Бояться не стоит, ведь такие менеджеры паролей всегда имеют мощный механизм шифрования (например,

AES шифрование). Наиболее популярные менеджеры паролей: Dashlane, KeePass, 1Password, LastPass, Kaspersky Password Manager [4].

- Биометрическая аутентификация. *Биометрическая аутентификация* – процесс подтверждения личности, с помощью предъявления своих биометрических данных. Биометрическая аутентификация отличается от других способов подтверждения личности тем, что использует биологические особенности человека. Самые распространённые технологии биометрической аутентификация – это отпечаток пальца, радужная оболочка глаза, геометрия лица, голос. К «экзотическим» технологиям можно отнести: термограмму лица, рукописный почерк, ДНК, сердечный ритм, особенности набора текста на клавиатуре [4].
- Смарт-карты или USB-токены. *Смарт-карта/USB-токен* – это внешний носитель информации, который применяется при аутентификации пользователя. Аутентификацию с помощью смарт-карт или USB-токенов сложнее обойти, так как используется уникальный физический объект, на котором содержится сертификат и секретный ключ. К каждому физическому носителю необходимо дополнительно ввести секретный PIN-код, что значительно повышает безопасность [2].

Соблюдение операторами и субъектами персональных данных мер по защите информации позволит уменьшить риск утечки конфиденциальной информации в несколько раз.

## Исследование

Проведенное исследование направлено на определение уровня осведомлённости граждан в области персональных данных.

Всего в исследование приняли участие 70 человек разной возрастной группы.

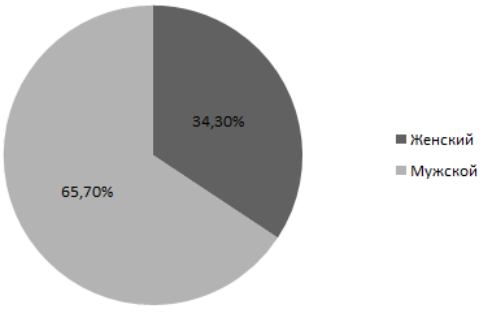



*Рис. 1. Половой состав респондентов*

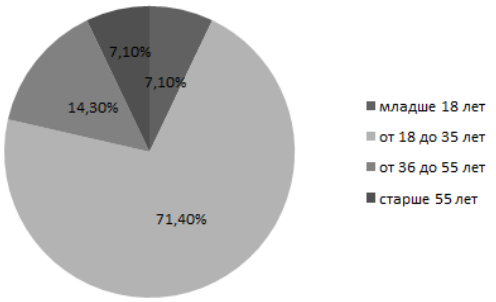



*Рис. 2. Возрастной состав респондентов*

Большинство респондентов (65.7%) знают, для чего используются персональные данные (рис. 3), 31% только догадываются, но точно для чего используются сказать не могут. Примерно в таком же соотношении респонденты знают, что именно относится к персональным данным (рис. 4). По данным результатам уже можно сделать промежуточный вывод, что люди понимают, что такое персональные данные.

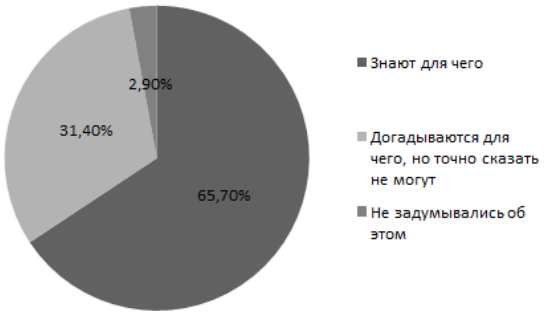



*Рис. 3. Процентное соотношение ответов на вопрос «Для чего используются персональные данные?»*


*Рис. 4. Процентное соотношение ответов на вопрос «Можете ли Вы привести пример персональных данных?»*

55.7% опрошенных знают о своих правах в общих чертах. 15.7% никогда не слышали, что государство как-то регулирует сферу персональных данных. 28.6% хорошо знают права и обязанности в сфере законодательства (рис. 5).

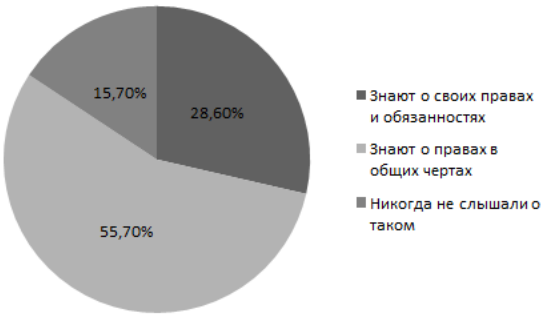



*Рис. 5. Процентное соотношение ответов на вопрос «Знаете ли Вы свои права и обязанности в области персональных данных?»*

При подписании согласия на обработку персональных данных только половина респондентов внимательно прочтут документ и подпишут. 13% сразу подпишут и не станут читать документ (рис. 6).


*Рис. 6. Процентное соотношение ответов на вопрос о подписании согласии на обработку персональных данных*

65.7% опрошенных сталкивались с незаконной обработкой персональных данных. Довольно высокий показатель. 42.9% никогда не читают текст политики конфиденциальности, а 44.3% – только основные пункты (рис. 7).

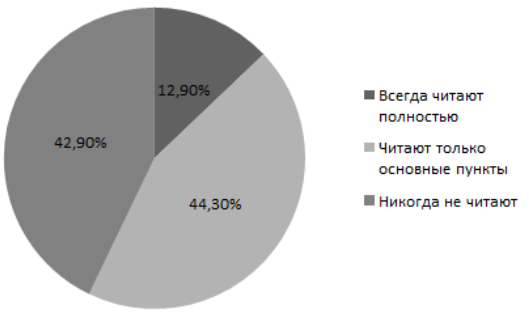



*Рис. 7. Процентное соотношение ответов на вопрос «Всегда ли читаете текст политики конфиденциальности?»*

Пользователи для защиты своих данных наиболее часто используют пароли (91.4%), PIN-код (71.4%), биометрические данные (75.7%). Реже используют двухфакторную аутентификацию (62.9%), менеджер паролей (21.4%).

Смарт карту или USB-токен в качестве защиты используют всего 2.9% опрошенных (рис. 8).

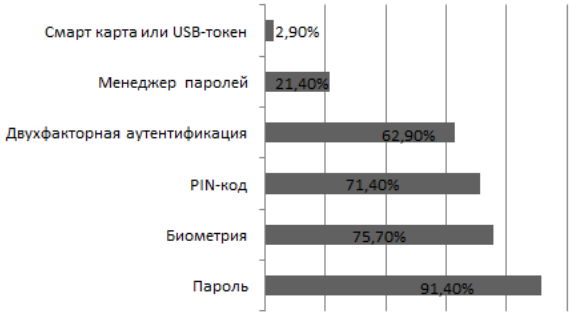



*Рис. 8. Наиболее частые способы защиты данных*

40% респондентов не доверяют свои данные «менеджеру паролей» – боятся, что данные будут украдены. 25.7% вообще не знаю, что такое «менеджер паролей» (рис. 9).

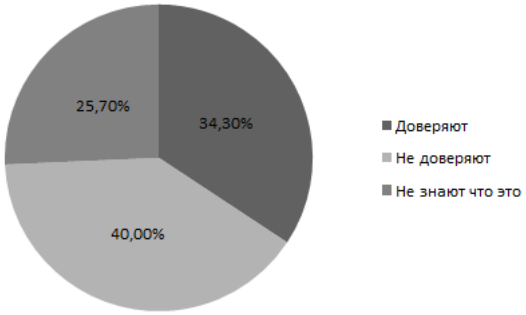



*Рис. 9. Процентное соотношение ответов на вопрос «Доверяете ли Вы свои данные Менеджеру паролей?»*

Большинство респондентов (59.4%) создают пароли повышенной сложности. 11.6% в качестве пароля используют дату рождения, имена и так далее (рис. 10).


*Рис. 10. Процентное соотношение ответов на вопрос о сложности создаваемых паролей*

58.6% обновляют свои пароли только после утечки данных, или когда забывают этот пароль. 21.4% обновляют один раз в 6 месяцев, 18.6% – один раз в год (рис. 11).

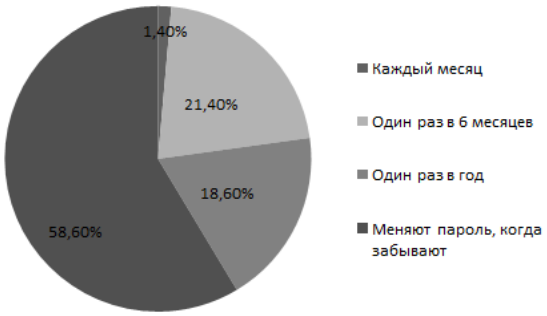



*Рис. 11. Процентное соотношение ответов на вопрос о частоте обновления паролей*

Аккаунты в социальных сетях или мессенджерах у 63.8% респондентов подвергались взлому (рис. 12).

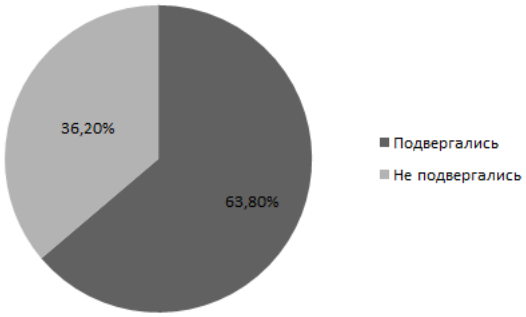



*Рис. 12. Процентное соотношение ответов на вопрос «Подвергались ли Ваши аккаунты в соц. сетях взлому?»*

62.9% сталкивались с попыткой вымогательства персональных данных, а 10% стали жертвами мошенников (рис. 13).

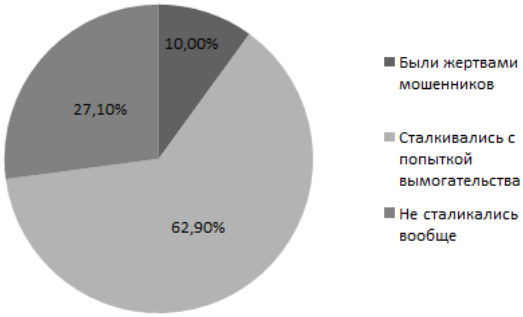



*Рис. 13. Процентное соотношение ответов на вопрос «Сталкивались ли Вы с попыткой вымогательства?»*

42.9% считают, что основной причиной утечек данных – это безответственность и небрежность к передаче своих данных. 30% винят операторов персональных данных – злоупотребление и разглашение данных клиентов. 15.7% в качестве причины назвали недостаточно высокий уровень развития технологий по защите данных, а 11.4% – слабое законодательство в сфере персональных данных (рис. 14).

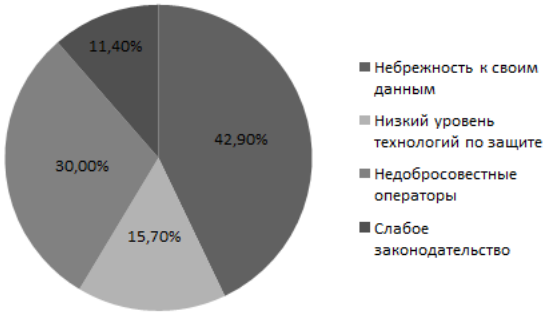



*Рис. 14. Причины утечек персональных данных*

55.7% стараются защищать свои данные, а 44.3% скрывают свои данные (рис. 15).


*Рис. 15. Процентное соотношение ответов на вопрос «Вы скрываете или защищаете свои данные?»*

По результатам проведенного исследования можно сделать следующий вывод. Уровень осведомленности граждан в сфере персональных данных чуть выше среднего. Люди не очень заинтересованы в защите своих данных. Большинство людей не станут интересоваться тем, как их данные будут обрабатываться, кто их будет обрабатывать, куда данные будут перенаправлены. Мошенники все также пытаются выкрасть персональные данные, и у них это неплохо получается – больше половины опрошенных были жертвами мошенников. Старшее поколение ответственно подходит к правам и обязанностям в сфере персональных данных, но реализация защиты данных – большая проблема. Молодежь, наоборот, боле ответственно подходит к вопросу реализации защиты.

**Решение данной проблемы**

В цифровую эпоху персональные данные пользователей имеют значительную ценность для злоумышленников. Большинство утечек и атак, зачастую, происходят с одной целью – получение денежной прибыли.

Исследование и изучение материалов по данной теме показали, что к нарушению конфиденциальности персональных данных приводят следующие действия:

- Низкий уровень информационной и цифровой образованности населения
- Безответственность субъектов в области защиты свои данных
- Нет понимания о необходимости защищать свои данные
- Злоупотребление полученными данными стороной, которая имеет доступ к персональным данным и занимается их обработкой

Я считаю, что в качестве решения данных проблем нужно разъяснить необходимость выполнения правовых актов, направленных на ответственное отношение к личным данным, среди школьников, молодежи, сотрудников организаций, граждан старшего поколения. Необходимо объяснить, в чем ценность персональных данных, какие бывают последствия от утечки и как защитить данные. Также необходимо адаптировать тексты правовых документов с юридического языка на обыденный язык. Активно в образовательных и государственных организациях проводить лекции, «открытые» уроки, мастер-классы, тренинги, игры, конкурсы, семинары на данную тему. Необходимо создать единое, молодежное, медийное Интернет-пространство для популяризации защиты персональных данных и поднятии уровня цифровой грамотности. Обеспечить беспрепятственную консультацию по вопросам защиты данных с регуляторами персональных данных.

Считаем, что необходимо реформировать законодательство в сфере персональных данных. Реформирование улучшит правовую защиту данных граждан. Необходимо пересмотреть следующие пункты в законодательстве:

- Наказание за неправомерное использование персональных данных. Я считаю, что нужно ужесточить наказание за незаконное использование чужих данных. На данный момент злоумышленники почти не ощущают строгость наказания (очень маленькие штрафы, до 50 тысяч рублей).
- Аттестация информационных систем персональных данных. На законодательном уровне поднять качество проведения аттестационных испытаний для подтверждения соответствия требованиям информационной безопасности. Также для частных организаций, как и для государственных, установить обязательное прохождение аттестации ИСПДн.

- Правовой статус оператора персональных данных. Ужесточить проверку для получения статуса оператора персональных данных. На данный момент большое количество недобросовестных операторов. Операторы очень часто «сливают» данные или используют их в незаконных целях.
- Сертифицирование аппаратных и программных продуктов. Увеличение количества сертифицированных программных и аппаратных продуктов снизит риски утечки персональных данных [11].

Создание международных и региональных соглашений по защите персональных данных также помогут решить некоторые проблемы. Соглашения помогут разным государствам и национальным регионам делиться положительным или отрицательным опытом в сфере персональных данных.

Считаю, что для поддержания и совершенствования области защиты персональных данных нужно укрепить роль Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в этой сфере. Укрепление роли данного регулятора даст повышение эффективности в разработке новых методик противодействия нарушениям против персональных данных.

Главное решение проблемы конфиденциальности персональных данных – это четкое понимание о необходимости ответственного и бережного обращение, как к своим данным, так и к чужим. Люди должны осознать всю ценность личных данных и возможные от утечки последствия для самого владельца и всего общества в целом.

## Список литературы

1. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. Учебное пособие, 2018
2. Шаньгин В.Ф. Информационная безопасность и защита информации. Учебное пособие, 2019
3. Прохорова О.В. Информационная безопасность и защита информации. Учебное пособие, 2014
4. Скрипник Д.А. Обеспечение безопасности персональных данных. Учебное пособие, 2020
5. Исаев А.С., Хлюпина Е.А. Правовые основы организации защиты персональных данных, 2014
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
7. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»

8. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 18.02.2009 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»

9. Приказ ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

10. Приказ ФСТЭК от 18.02.2013 № 32 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

11. [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации URL: https://digital.gov.ru (дата обращения: 01.03.2022)

12. [Электронный ресурс] // Персональные данные, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций URL: https://rkn.gov.ru/personal-data/ (дата обращения: 25.03.2022)

13. [Электронный ресурс] // Документы Федеральной службы по техническому и экспортному контролю URL: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam (дата обращения: 03.04.2022)

## PRIVACY OF PERSONAL DATA

***N.A. Shardakov, M.Yu. Karpov***
Perm State National Research University

**Abstract.** Within the framework of the research work on the topic «Confidentiality of personal data» the urgency of the problem of personal data confidentiality is proved. The main problematics of this article is: violation of data confidentiality. The purpose of this article is to find out what is personal data, by what means the confidentiality of personal data is maintained, the main causes of data leakage, ways of protection. Objectives of this article – to consider the main causes of personal data leakage and their consequences, to propose a solution to this problem. As a proof of the relevance of the problem, the results of the survey are presented, the purpose of which is to identify the level of awareness of citizens in the field of personal data.
**Keywords:** *personal data, confidentiality, protection, leakage, information, consequences, reasons, legislation.*

# ПОПУЛЯРИЗАЦИЯ РОССИЙСКОЙ КУЛЬТУРЫ

***Ю.М. Шадрина, Д.Р. Бакирова, Е.П. Брюхова, Е.Ю. Никитина***
Пермский государственный национальный исследовательский университет

**Аннотация**. Данная статья посвящена одному их способов противодействия деструктивному воздействию на человека через популярную культуру. Воздействие на психику и мировоззрение молодежи посредством массовой культуры является одним из самых эффективных методов воздействия и очень часто используется для достижения целей недоброжелателями. К сожалению, на сегодняшний день в России данная проблема активно не решается. Рассмотренный метод в какой-то мере способен, по мнению авторов, противодействовать деструктивному влиянию на молодое поколение. Заключается он в воспитании любви к культуре России, знакомстве молодежи с творчеством российских авторов, формировании положительного восприятия к массовой культуре России.
**Ключевые слова**: *деструктивное воздействие, средства противодействия, информация, общество, человек, социальные сети, культура, творчество, российская культура, массовая культура.*

## Введение

Мы живем в развивающемся информационном обществе. Основным ресурсом в нем является информация. С развитием информационных технологий, социальных сетей, телевидения, СМИ, телекоммуникаций ее получение стало легкодоступным, что приводит к тому, что человек получает информацию в огромных количествах. В этом есть свои плюсы, но и минусов множество, таких как: информационная перегрузка, нарушение обучения и восприятия информации, снижение концентрации внимания, развитие хронического стресса и, конечно, потеря способности критически мыслить и оценивать окружающую обстановку.

Последнее возникает в результате деструктивного воздействия информации на человека. Сущность такого воздействия в скрытом принуждении личности принимать чужие взгляды как свои собственные, принимать решения и осуществлять конкретную практическую деятельность, выгодные тем, кто осуществляет такое информационное воздействие.

Главное во всех этих процессах – преобразование сознания каждой личности, социокультурных регуляторов ее жизнедеятельности и формирование положительного отношения к содержанию предлагаемой социальной информации и к тем, кто осуществляет такое информационное воздействие [1]. Результат такого процесса – это ограничение свободы воли, принятия собственных решений человеком, изменение состояния общества и государства. В связи с последними событиями, информационное воздействие на население Россий-

ской Федерации активно используется для формирования общеполитической ситуации в стране.

К сожалению, уровень обычной грамотности не помогает эффективно распознать опасность, скрытую в доносимой до людей информации. Это приводит к незащищенности широких слоев населения, в первую очередь молодого поколения, от негативного информационного влияния.

## Методы воздействия

Существует множество способов и методов информационного влияния на человека. Самыми распространенными из них являются:

1) Секты, в которых осознанно вырабатывается зависимость человека от данного сообщества и происходит лишение его автономии
2) Пропаганда различного рода
3) Романтизация нездорового образа жизни с помощью сериалов, телешоу, фильмов и прочего
4) Распространение пугающих новостей, видеоматериалов, псевдоисследований, лекций псевдоученых через СМИ, форумы и социальные сети

Одним из самых эффективных способов воздействия на молодежь является воздействие через популярную культуру. Несколько последних десятилетий он активно используется по всему миру, в том числе и в России. И, к сожалению, серьезного противодействия ему не осуществляется.

## Методы противодействия

Существует множество способов противодействия негативному информационному влиянию, такие как нормативное регулирование, цензура, модерация сетей и блокировка источников, социальная реклама, психологические тесты, родительский контроль, прививание жизненных ценностей в школах и т.п.

Рассматриваемый в данной статье способ ориентирован на противодействие деструктивному воздействию на подростков и молодых людей нашей страны через популярную культуру. По наблюдениям авторов, уже существующие методы в основном заключается в блокировке контента или определенных ресурсов, что на деле оказывается не полностью эффективным. Предлагаемый же способ заключается в борьбе с существующим среди молодого поколения мнением о культуре в РФ и взглядах на жизнь в целом.

Из проведенных наблюдений в социальных сетях [2] и личного общения с молодежью, можно сделать вывод, что большинство молодых людей считают культурную сферу России отсталой и находящейся в упадке, при том, что многие даже ни разу не видели фильмов российского и советского производства,

почти не читали книг. Мало кто задумывается над потребляемым контентом и над тем, какие ценности им прививает популярная культура.

При таких уже устоявшихся и распространенных взглядах запреты и блокировки бесполезны. Необходимо не запрещать негативный контент, а прививать любовь к положительному.

**Возможное решение**

Идея предлагаемого способа решения проблемы заключается в воспитании у молодого населения России любви к культуре нашей страны, в раскрытии для них культурной ниши России, знакомстве с произведениями искусства. Осуществляться это будет посредством трансляции молодому населению творчества деятелей искусства РФ, СССР и досоветских времен посредством социальных сетей и при личном общении.

Реализация идеи в социальных сетях включает в себя создание групп в ВКонтакте и Телеграмм, в которых публикуются тематические подборки со ссылками на ресурсы с фильмами, сериалами и мультфильмами, посты о книгах российских писателей, статьи об интересных российских и советских авторах, художниках, композиторах, режиссерах, исполнителях и актерах, плейлисты с музыкальными подборками, викторины и тесты. Так же в этих группах будут предусмотрены чаты, в которых можно будет обсуждать уже просмотренное или прочитанное.

Данная идея базируется на психологическом воздействии через общение. Воздействие всегда реализуется в процессе общения, будь то обычный разговор, или – в случае манипулирования общественным мнением, – в прослушивании лекции, или же в форме прочтения какого-либо текста.

Традиционно выделяются четыре основных способа влияния: убеждение, внушение, заражение и подражание. В реализации идеи в социальных сетях используются такие методы влияния, как заражение, убеждение и внушение.

Феномен заражения возникает у людей, которые руководствуются в поведении своим эмоциональным состоянием. Используя такие невербальные средства, как музыка, фильмы, сериалы и т.п. происходит воздействие на человека. Стоит отметить, что заражение основывается на общем переживании группой людей одних и тех же эмоций и носит спонтанный характер.

Убеждение включает в себя систему доводов, которые обосновывают выдвигаемое пожелание. В результате обсуждения в чате убеждение ведет к трансформации взглядов человека. При этом, убеждение основано на осмысленном принятии человеком каких-либо решений и идей.

Внушение, как и убеждение, направлено на снятие своеобразных фильтров у людей. Внушение вызывает представления об идее так, как если бы эти

представления были получены непосредственно человеком, на которого это внушение осуществляется. Этот метод носит эмоционально-волевой характер и основывается на доверии. При внушении действуют специфические социально-психологические факторы. Решающим условием эффективности данного метода будет являться авторитет человека, внушающего идею.

Реализация предлагаемого решения на практике представляет собой создание клубов в учебном заведении, в которых могут проводиться встречи любителей российской культуры, литературные и костюмированные вечера, чаепития, совместные просмотры фильмов и их обсуждения. Так же члены клубов могут проводить встречи с остальными учащимися, знакомить их с культурой России, обсуждать с ними различные произведения, узнавать их мнение и при необходимости корректировать, используя те же методы влияния, которые были описаны выше.

Также в качестве метода влияния в реализации можно использовать подражание. Этот метод заключается в следовании примеру или образцу, которое проявляется в повторении одним человеком каких-либо поступков, жестов, черт характера другого человека. Подражание может носить произвольный и непроизвольный характер. Стоит отметить, что в разные возрастные периоды подражание играет в жизни человека неодинаковую роль. То есть, в младшем возрасте подражание будет более эффективно, чем в старшем.

В настоящее время реализация предложенного решения выполнена в виде сообществ в социальных сетях ВКонтакте и Телеграмм под названием «Сила в искусстве» (рис. 1). В группе ВКонтакте публикуются различные материалы на тему российской и советской культуры.


*Рис. 1. Заглавный пост сообщества*

Контент сообщества поделен по дням недели:

1) Понедельник – день художественного искусства;
2) Вторник – день литературы;
3) Среда – день поэзии;
4) Четверг – день музыки;
5) Пятница, суббота – дни кино;
6) Воскресенье – день мультфильмов.

В каждый из дней недели подписчики группы знакомятся с разнообразными произведениями и авторами российской культуры. Сначала происходит знакомство с автором через небольшую статью о его деятельности и жизни (рис. 2).

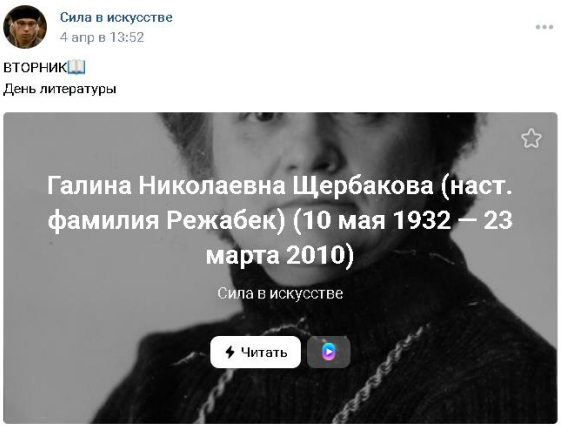



*Рис. 2. Статья о Г.Н. Щербаковой*

После прочтения статьи идет несколько постов с работами этого автора (рис. 3).


*Рис. 3. Экранизация повести Г.Н. Щербаковой «Вам и не снилось»*

Выше был пример дня литературы. Формирование информации в остальные дни происходит аналогичным образом.

По отзывам пользователей, одним из самых интересных дней был день художественного искусства. Иллюстрации Ивана Яковлевича Билибина к русским сказкам (рис. 4), знакомые многим с детства.


*Рис. 4. Иллюстрации И.Я. Билибина к сказке «Василиса Премудрая»*

Наиболее эффективными в продвижении видов контента являются ВК-Клипы. Это красивые или смешные короткие видео по различным произведениям кинематографа, таким как «Ну погоди!», «Морозко», «Мой ласковый и нежный зверь», «Ученик лекаря» и другие (рис. 5).


*Рис. 5. ВК-Клипы в сообществе «Сила в искусстве»*

В Телеграмм канале «Сила в искусстве» дублируется информация из ВКонтакте для большего охвата аудитории.

Реализация клуба в реальной жизни была реализована частично в форме занятий с учащимися младших курсов ПГНИУ кафедры информационной безопасности и систем связи. Было проведено два занятия на тему российского кинематографа. На первом занятии была показана презентация с кадрами из популярных российских и советских фильмов, обсуждение российского и советского кино. На втором занятии состоялся просмотр фильма «Вам и не снилось» (рис. 6).

*Рис. 6. Второе занятие со студентами*

В заключении стоит отметить, что предложенный авторами способ решает в определенной мере поставленную проблему деструктивного воздействия информации на человека. Этот способ неявный, несложный для восприятия конечным пользователем, а также достаточно легкий с точки зрения его реализации.

**Список источников**

1. Нечевин Д.К. «Правовое регулирование деструктивных информационных воздействий, оказывающих негативное влияние на формирование психосферы человека»

2. [Электронный ресурс] Общение как основа психологического воздействия https://otherreferats.allbest.ru/psychology/00105222_0.html?ysclid=lgsby1dfti938865601

## POPULARIZATION OF RUSSIAN CULTURE

***Y.M. Shadrina, D.R. Bakirova, E.P. Bryukhova, E.Yu. Nikitina***
Perm State National Research University

**Abstract.** This article is devoted to one of the ways of counteraction to destructive influence on a person through popular culture. Influence on the psyche and worldview of young people through popular culture is one of the most effective methods of influence and is very often used by ill-wishers to achieve their goals. Unfortunately, to date in Russia this problem is not actively addressed. The considered method to some extent is able, according to me, to counteract the destructive influence on the young generation. It consists in education of love to culture of Russia, familiarization of youth with creativity of Russian authors, formation of positive perception to mass culture of Russia.
**Keywords:** *destructive influence, means of counteraction, information, society, man, social networks, culture, creativity, Russian culture, mass culture.*

# МОДЕЛИРОВАНИЕ МАСКИРОВКИ ЭМОЦИОНАЛЬНОГО ПОСЫЛА ГОВОРЯЩЕГО ЧЕЛОВЕКА ЗА СЧЕТ СУПЕРПОЗИЦИИ ИСХОДНОЙ ЗВУКОВОЙ ВОЛНЫ СПИКЕРА И ВОЛНЫ, СОДЕРЖАЩЕЙ ЗАДАННЫЙ ЭМОЦИОНАЛЬНЫЙ ПОСЫЛ

***А.П. Шкарапута***
Пермский государственный национальный исследовательский университет

**Аннотация**. В данной работе, с целью сокрытия эмоций, содержащихся в голосе человека, предлагается накладывать на звуковую волну, воспроизводимую говорящим человеком, еще одну звуковую волну с другим доминирующим эмоциональным посылом. Приводятся возможные сферы деятельности, в которых требуется маскировка эмоционального состояния. Дана оценка применимости метода отношения локальных максимумов частот спектра исходной звуковой волны для быстрого распознавания эмоций и генерации накладываемого маскирующего сигнала.
**Ключевые слова**: *эмоции, звуковая волна, эмоциональный посыл, эмоциональное состояние, маскирующий сигнал*.

## Введение

В настоящее время существует множество работ по распознаванию эмоционального состояния человека, используя характеристики звуковой волны его голоса. Авторы соревнуются по созданию методов и программ на их основе для распознавания эмоций. Хотя есть разные взгляды на классификацию эмоционального состояния человека, в частности, можно рассматривать их категории дискретно или водить какую-то непрерывную шкалу, все же уже суще-

ствуют программные продукты, позволяющие распознавать эмоцию человека по голосу. Также ведутся работы по эмуляции эмоционального посыла.

Задача маскировки эмоционального состояния может иметь большую актуальность, потому что проявление эмоций несет информацию о говорящем и его отношении к тому, о чем он говорит, однако, в большинстве случаев, проявление эмоций иррационально и не подконтрольно. Иногда нужно изменить голос человека, для сохранения его инкогнито. В этом случае легко изменяется тембр и некоторые другие характеристики, но эмоциональная составляющая, как правило, остается и несет информацию о манере поведения человека.

С точки зрения информационной безопасности задача маскировки эмоционального состояния связана с конфиденциальностью информации, причем информации, не связанной с лексемами речи, а связанной с другой ее составляющей – просодией. Маскировка эмоций может быть применена во множестве случаев, от телевизионных шоу до использования в судебной системе.

В данной работе для маскировки эмоционального посыла есть вариант наложить на исходную звуковую волну сигнал, который не изменит содержание речи, но придаст результирующему звуку другую эмоциональную окраску, в том числе, и бесцветную. Для создания маскирующего сигнала, зависящего от исходной звуковой волны, предлагается использовать метод отношения частот локальных максимумов спектра [1].

Оценена сложность задачи сокрытия эмоционального состояния как в режиме реального времени, так и в результате обработки записей.

## Метод отношения частот локальных максимумов применительно к маскировке эмоционального состояния

Для сокрытия эмоций в голосе с помощью добавочного сигнала требуется не просто накладывать сигнал, эта добавка не должна выглядеть инородной. Добавочная волна должна зависеть от исходной звуковой волны говорящего, и, по сути, перед модификацией необходимо сначала определить вначале ее эмоциональный посыл.

Есть различные подходы для создания классификаторов, с помощью которых распознаются эмоции. Однако для модификации звука требуется не просто иметь классификаторы, нужно, чтобы эти классификаторы отражали «природу» эмоционального посыла, так как необходимо понимать, что нужно менять… Так, использование, например, мел-кепстральных коэффициентов [2] в качестве классификаторов, хорошо может быть применимо для распознавания эмоций, однако для модификации исходной звуковой волны они трудно применимы. Сложности могут быть и при применении методов искусственной нейронной сети, так как она во многом работает как «черный ящик», где на

входе исходный сигнал, на выходе эмоция. Поэтому необходим метод, классификаторы которого улавливают природу эмоциональной окраски.

Здесь предлагается к рассмотрению метод, который основан на использовании в качестве классификаторов отношения частот локальных максимумов. Суть метода заключается в том, что на секторальной зависимости, представленной условно на рисунке 1 (где A – амплитуда, а f – частота звуковой волны) определяются локальные максимумы, а затем, вычисляются отношения соответствующих им частот.

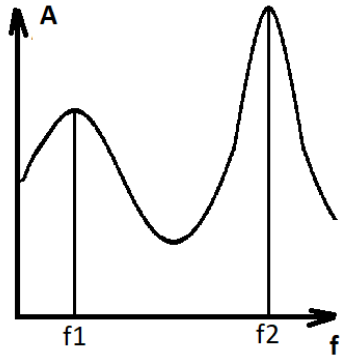



*Рис. 1. Спектральная зависимость звуковой волны (амплитуды A от частоты f) с выделенными локальными максимумами f1 и f2*

Для рассматриваемого примера отношение частот двух локальных максимумов – это

$$Ratio=f1/f2.$$

В реальном спектре зависимости намного сложнее и проявляется множество локальных максимумов, для которых можно построить большое количество отношений, что дает различную информацию об эмоциональной окраске, в том числе о притворстве говорящего.

Приведенный метод хорошо отражает «природу» эмоционального посыла. Так, нужно отметить, что отношения частот хорошо сочетаются с музыкальными интервалами. и отношение 0,79 соответствует большой терции и, чаще всего находилось в речи с радостной эмоциональной окраской (это первый интервал мажорного аккорда), а отношение 0,84 соответствует малой терции и, чаще всего находилось в речи с печальной окраской (это первый интервал минорного аккорда). Отношения частот удобнее использовать по сравнению с применением простых частот тем, что говорящий может говорить выше или ниже, быстрее или медленнее, сохраняя эмоциональную окраску, частоты при этом изменяются, а вот отношение частот не изменяются. Суть маскировки эмоционального состояния на основе рассматриваемого метода будет заключаться в том, что поверх исходного звука можно наложить волну, содержащую необходимые (другие, которые будут доминирующими) отношения частот.

**Возможности и ограничения метода отношения частот локальных максимумов для маскировки эмоционального состояния**

В работе [3] на основе 60-ти фрагментов записей (по 10 на базовую эмоцию) были определены наиболее часто встречаемые отношения частот при разных эмоциональных состояниях (Гнев 0.69, Страх 0.74, Отвращение0.67, Удивление 0.50, Печаль 0.84, Радость 0.79), также показано, что при использовании в качестве классификаторов в том числе и других отношений (не только наиболее часто встречающихся) локальных максимумов, можно с помощью метода искусственной нейронной сети довольно точно разделить записи по категориям эмоций.

Таким образом, имеется некоторая теоретическая основа для распознавания эмоционального состояния и внесения изменений в исходную звуковую волну.

На рис. 2 представлен реальный спектр звуковой волны, содержащей радостную эмоцию. Здесь локальные максимумы отмечены красными точками, кроме того, в выделенном красным прямоугольнике фрагменте показано, как мог бы измениться спектр при добавлении внешнего звукового сигнала, создающего новые локальные максимумы.

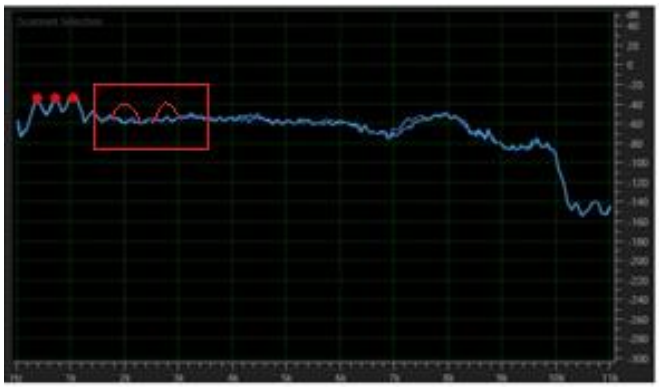


*Рис. 2. Спектр звуковой волны, содержащей радостную звуковую окраску с добавлением внешнего звукового сигнала*

Маскировка звука может проводиться в двух режимах: в режиме реального времени, когда необходимо вносить изменения в голос непосредственно во время его воспроизведения и в режиме редактировании записи.

При маскировке в режиме реального времени использование метода отношения частот локальных максимумов требует организации задержки воспроизведения искаженного сигнала, не менее чем на 1 секунду. Дело в том, что локальные максимумы, с большей точностью отражающие эмоциональный посыл, лучше всего находятся на фрагментах звука в 1 секунду. Возможно наложение добавочного сигнала и без предварительного распознавания эмоционального посыла, но в этом случае не будет возможности выбора участка спектра, в который нужно вносить искажения.

Также, были проведены сравнения записей людей с искренними эмоциями и людей их имитирующих. Было обнаружено, что во всех случаях, когда человек имитировал эмоцию в звуковой волне проявлялось отношение частот локальных максимумов 0,75, характерное для чистой квинты (соответствует «пустому звучанию»). Таким образом, имеется вариант, при котором для придания нейтральности или неискренности эмоций, можно добавлять в исходную звуковую волну сигнал, содержащий чистую квинту.

Внесение дополнительного сигнала можно осуществить, например, используя амплитудное преобразование, когда значения семплов звука исходной звуковой волны, полученных в результате дискретизации звука, складываются с соответствующими величинами добавочного сигнала.

## Заключение

Модификация эмоционального состояния человека путем наложения на его речь дополнительного сигнала может иметь большие перспективы в разных сферах деятельности человека. Рассматриваемый подход является «по сути» первым приближением для изменения эмоциональной окраски и, скорее всего, будет пригоден именно для маскировки испытываемой эмоции, а не для замены ее на другую, таким образом, чтобы слушатели этого не заметили. Для того, чтобы маскирующий сигнал не стал обычным фоновым звуком, необходимо учитывать различные факторы. Очевидно, что эмоциональная окраска зависит от множества параметров: вибрации, придыхания, повышение тона и прочих параметров [4,5]. Эти параметры также могут влиять на маскирующий сигнал и предложенный метод может быть использован как в сочетании с другими подходами, так и в отдельности.

## Список литературы

1. Близнюк О.А., Шкарапута А.П. Исследование применения метода определения базовых эмоций на основе отношения частот спектра звуковой волны Научный журнал «Вестник пермского университета». Математика. Механика. Информатика. 2017. Выпуск 4(39) С. 86-91

2. Xuedong, H. Spoken Language Processing: A Guide to Theory, Algorithm and System Development. Huang Xuedong. New Jersey. Prentice Hall PTR (2001).

3. Shkaraputa, A., Kolcherina, A., Mishlanova, M. (2022). Determining of the Emotional State of a Person Using Computer Analysis of Sound Wave Parameters. In: Rocha, A., Isaeva, E. (eds) Science and Global Challenges of the 21st Century – Science and Technology. Perm Forum 2021. Lecture Notes in Networks and Systems, vol 342. Springer, Cham. https://doi.org/10.1007/978-3-030-89477-1_6

4. Романенко В.О. Эмоциональные характеристики вокальной речи и их связь с акустическими параметрами [Текст] / Романенко В.О. // Terra Humana. – 2011. – № 124

5. Ильин Е.П. Эмоции и Чувства. СПб.: Питер, 2001. 752 с.

## MODELING OF MASKING THE EMOTIONAL MESSAGE OF A SPEAKING PERSON DUE TO SUPERPOSITION OF THE SPEAKER'S INITIAL SOUND WAVE AND THE WAVE CONTAINING A GIVEN EMOTIONAL MESSAGE

***A.P. Shkaraputa***

Perm State National Research University

**Abstract**. In this paper, in order to conceal emotions contained in a person's voice, it is proposed to superimpose another sound wave with a different dominant emotional message on the sound wave reproduced by a speaking person. Possible spheres of activity in which masking of emotional state is required are given. The applicability of the method of the ratio of local maxima of frequencies of the spectrum of the initial sound wave for quick recognition of emotions and generation of the superimposed masking signal is evaluated.

**Keywords:** *emotions, sound wave, emotional message, emotional state, masking signal.*

## ПОИСК ОПТИМАЛЬНЫХ РЕШЕНИЙ ДЛЯ МОДИФИКАЦИИ ЗВУКОВОЙ ВОЛНЫ ГОВОРЯЩЕГО ЧЕЛОВЕКА С ЦЕЛЬЮ СОКРЫТИЯ ЕГО ЭМОЦИЙ

***А.П. Шкарапута, Н.Ю. Ротанева, И.В. Сагиров***

Пермский государственный национальный исследовательский университет, Мариупольский государственный университет имени А.И. Куинджи

**Аннотация**. В работе рассматривается вопрос поиска оптимального решения для модификации звуковой волны голоса человека для изменения ее эмоционального посыла. В качестве такого решения предлагается применение фильтрации: за счет ослабления одной части спектра звуковой волны и усиления другой ее части. Сокрытие эмоций может быть актуальной задачей в социальных системах и может приводить как к положительным, так и отрицательным последствиям, в частности, создания фальшивок. Поэтому, кроме проблемы конфиденциальности, которую может обеспечить маскировка эмоции (значит и маскировка манеры поведения говорящего), рассматривается также проблема целостности и аутентичности информации, содержащейся в звуковой волне. Приведены возможные способы внесения таких изменений в звуковую волну говорящего, которые впоследствии помогали бы установить сам факт модификации звука, и приведено сравнение этих способов для поиска лучшего из них.

**Ключевые слова***: звуковая волна, эмоциональный посыл, сокрытие эмоций*.

## Введение

Эмоции – это неотъемлемая часть человеческого общения и передачи информации, причем передача эмоционального посыла один из наиболее древних способов донесения информации, при этом звуковая ее форма является более социальным явлением, так как в отличие от мимики и жестов может передаваться на большие расстояния, использоваться в любое время суток и не только в зоне прямой видимости.

Эмоции являются характерной чертой каждой конкретной личности, определяющих его манеру поведения и отношение к происходящему. Так как эмоциональное поведение иррационально и слабо поддается контролю, то в связи с этим возникает проблема маскировки эмоционального посыла или, даже, его изменения. Данная проблема не только связана с задачей конфиденциальности информации, (так как от непосвященных скрывается истинный эмоциональный посыл), но и связана с ее целостностью и аутентичностью. Любой метод модификации информации может использован в самых различных целях. Например, можно изменить голос человека на телевизионном шоу для сокрытия говорящей личности, а можно придать голосу политика на выборах неподобающую интонацию. Очевидно, что при использовании модификации информации имеют место две тенденции: стремление произвести изменения так, чтобы они выглядели наиболее естественным образом и стремление различить подлинную информацию и измененную. В связи с этим, перед создателями библиотек и программных продуктов, модифицирующих информацию, может стоять задача внесения водяных знаков, позволяющих судить о характере изменений.

Необходимо отметить, что задача распознавания эмоций является непростой во многих смыслах, начиная с применения различных моделей классификации эмоций и применения большого набора классификаторов (или небольшого набора, но сложных классификаторов). Задача эмулирования эмоций, для придания, например, читаемому роботом тексту большей естественности, также не является простой, но очевидно, что задача изменения существующего эмоционального посыла – это еще более сложная задача, так как нужно убрать старую эмоциональную окраску и естественным образом присоединить новую.

Рассмотрим акустические преобразования, которые можно осуществить при модификации звуковой волны. Изменение звука может происходить разными способами, один из простейших способов – это амплитудное преобразование. Изменения амплитуды звуковой волны несложно добиться, модифицируя уровни отсчетов (семплов) по определенному закону. Например, уменьшив значения всех семплов пропорционально некоторой величине, мы можем повысить или понизить общую громкость звука. Многие авторы сходятся во мнении,

что среди акустических характеристик, которые можно соотнести с базовыми эмоциями, одними из самых важных являются энергия и громкость [1].

Также, при амплитудных преобразованиях, можно величину семплов исходной волны складывать с величиной некоторого сигнала, в этом случае результатом будет суперпозиция исходной волны и добавочного сигнала. Здесь возникает трудность в конструировании подобного сигнала, определении временной точки его использования и другие моменты.

Одним из популярных способов преобразования звука является его модификация с помощью дискретного преобразования Фурье [2]. По исходным дискретным величинам громкости, которые получены в результате аналого-цифрового преобразования, строится спектральная картина (амплитудно-частотная зависимость), а дальше увеличиваются или уменьшаются амплитуды у интересующих частот, после чего выполняется обратное преобразование.

Предположим, что основной характеристикой, соотносящейся с эмоциональной окраской голоса (как минимум, для базовых эмоций), является отношение частот локальных максимумов [3], которые хорошо коррелируют с музыкальными интервалами теории музыки. Поэтому, для подавления частот, соответствующих доминирующим отношениям частот локальных максимумов, и внесения частот, соответствующих отношениям «искусственной» эмоции, необходим метод, связанный с частотными преобразованиями, в частности, дискретное преобразование Фурье.

## Подходы к модификации звука с целью изменения его эмоциональной окраски

Необходимо отметить, что эмоции человек выражает на б*о*льших временных промежутках, чем требуется для воспроизведения звуков речи. Так, например, сообщение «вау!» с базовой эмоцией «удивление» несет в себе информацию о трех звуках. Поэтому, как правило, для эмоций требуется намного больше классификаторов, чем для лексем, или они являются более сложными. В статье [4] показано, что для определения эмоциональной окраски по методу отношения частот локальных максимумов лучшим размером временного интервала является 1 секунда. Там же показано, что чаще всего для эмоции удивления встречается отношение 0,5, что соответствует музыкальному интервалу «октава».

Таким образом, для определения эмоций по заданному методу требуется 1 секунда. Как же теперь модифицировать звук с исходным эмоциональным посылом?

На первый взгляд достаточно разбить звуковую волну на фрагменты длительностью в 1 секунду, построить для каждого спектральную характеристику,

уменьшить амплитуды локальных максимумов частот доминирующих отношений и увеличить амплитуды частот тех локальных максимумов, которые соответствуют выбранной эмоциональной окраске. Как, например, схематично показано на рис. 1.

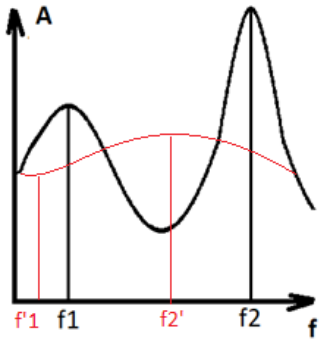



*Рис. 1. Спектральная зависимость исходной звуковой волны (амплитуды A от частоты f) с локальными максимумами f1 и f2 и модифицированной звуковой волны с локальными максимумами f1' и f2'.*

Однако, привнесенная новая частота распространится на весь фрагмент интервалом в 1 секунду. Тут возникает две проблемы: не совсем ясно, как она отразится на лексемах и в каких местах по времени должна именно проявляться внесенная частота. Так, в слове «вау» на первой гласной, например, была частота 220 (ля первой октавы), а у второй 110 (ля малой октавы), и, если мы хотим заменить интервал в октаву на интервал в большую терцию (соответствует радости с частотами 220 и 175), то в результате мы получим смесь одинаковых частот на каждой гласной букве. Ясно, что для данного примера нужно рассмотрение намного большего количества классификаторов, но для понимания процесса он хорошо подходит.

В результате, мы предлагаем следующий подход для решения этой проблемы. Для определения эмоциональной окраски необходимо использовать достаточно большие временные интервалы, а для внесения изменений с помощью дискретного преобразования Фурье эти временные интервалы нужно разбивать на более мелкие, настолько маленькие, чтобы не было искажений в лексемах. Далее на этих более мелких интервалах уже искать нужные частоты и, соответственно, вносить изменения.

## Проблема целостности и аутентичности информации

Как отмечалось ранее, имеется еще одна проблема, связанная с модификацией эмоционального посыла. В настоящее время становится актуальной проблема создания различных фальшивок, в том числе голосовых. Сейчас появляется возможность изменять голосовые сообщения конкретных людей или, даже, их генерировать. При этом, для придания звуку индивидуальных особен-

ностей, большую важность имеет манера общения конкретного человека, а не лексическое содержание речи. Поэтому, при создании программного обеспечения, позволяющего модифицировать звуковую информацию, в том числе изменить эмоциональный посыл, есть необходимость вносить водяные знаки.

Водяные знаки давно используются, например, для подтверждения авторства произведения. Один из вариантов их применения – запись поверх исходной звуковой волны какого-то другого тихого звука, однако такой подход легко вскрывается, кроме того, он портит качество записи. Другой подход – использование стенографических методов, например прятать информацию в метаданных файлов или вносить изменения в наименее значимые биты. Но эти подходы широко известны и применимы не для каждых форматов файлов; кроме того, такие «вставки» легко уничтожаются простым изменением форматов файлов. Поэтому, одним из лучших методов внесения водяных знаков может оказаться метод отношения частот локальных максимумов. То есть предлагается на определенном временном участке при модификации звука добиться того, чтобы отношения частот соответствовали нужным величинам – некому коду, причем эти отношения могут быть не обязательно доминирующими, а могут быть второстепенными. Такая модификация не будет меняться при изменении формата записи, изменениях уровня громкости и, даже, замедления или ускорения темпа воспроизведения. Устойчивость подобного подхода к изменениям громкости и скорости имеет общую природу с универсальностью использования метода отношений частот локальных максимумов спектра для определения эмоций, так как данные классификаторы не зависят от пола, возраста и, даже, национальности говорящего.

## Заключение

Модификация уже существующего эмоционального посыла в звуке является сложной задачей, в данной статье предложен подход для подобной модификации. Он основан на универсальных классификаторах – отношениях частот локальных максимумов спектра звуковой волны. Такие классификаторы хорошо отражают «природу» эмоциональной окраски и не зависят от множества факторов: высоты тона говорящего, скорости, громкости и прочих параметров. Поэтому изменение параметров для этого классификатора может оказаться одним из оптимальных решений.

Пока этот подход изложен на теоретическом уровне, но есть основания предполагать, что он сможет быть использован как самостоятельно, так и в сочетании с другими подходами. Также приведенный способ создания водяных знаков в звуковой волне может оказаться более универсальным, чем его использование для указания на существующее искусственное изменение эмоциональной окраски.

Работа выполнена в рамках научного проекта N1023030800002-3-1.2.1 «Системный анализ и принятие оптимальных решений в сложных технических, социально-экономических и образовательных системах (FRER – 2023-0001)».

## Список литературы

1. Mehmet Cenk Sezgin, Bilge Gunsel & Gunes Karabulut Kurt. Perceptual audio features for emotion detection. EURASIP Journal on Audio, Speech, and Music Processing volume 2012, Article number: 16 (2012)
https://doi.org/10.1186/1687-4722-2012-16

2. Волковец А.И., Дискретное преобразование Фурье. Спектр. [Электронный ресурс]. Режим доступа: https://www.bsuir.by/m/12_101945_1_116065.pdf (Дата обращения: 04.12.2023)

3. Близнюк О.А., Шкарапута А.П. Исследование применения метода определения базовых эмоций на основе отношения частот спектра звуковой волны Научный журнал «Вестник пермского университета». Математика. Механика. Информатика. 2017. Выпуск 4(39) С.. 86-91

4. Shkaraputa, A., Kolcherina, A., Mishlanova, M. (2022). Determining of the Emotional State of a Person Using Computer Analysis of Sound Wave Parameters. In: Rocha, A., Isaeva, E. (eds) Science and Global Challenges of the 21st Century – Science and Technology. Perm Forum 2021. Lecture Notes in Networks and Systems, vol 342. Springer, Cham. https://doi.org/10.1007/978-3-030-89477-1_6

## SEARCH FOR OPTIMAL SOLUTIONS FOR MODIFYING THE SOUND WAVE OF A SPEAKING PERSON IN ORDER TO CONCEAL HIS EMOTIONS

***A.P. Shkaraputa, N.Yu. Rotaneva, I.V. Sagirov,***
Perm State National Research University,
Mariupol State University named after A.I. Kuindzhi

**Annotation.** The paper deals with the question of finding an optimal solution for modifying the sound wave of human voice to change its emotional message. As such a solution the application of filtering is proposed: by weakening one part of the sound wave spectrum and strengthening the other part. Concealment of emotions can be an actual task in social systems and can lead to both positive and negative consequences, in particular, the creation of fakes. Therefore, besides the problem of confidentiality, which can be provided by emotion masking (hence masking the speaker's behavior), the problem of integrity and authenticity of the information contained in the sound wave is also considered. Possible ways of making such changes in the speaker's sound wave, which would later help to establish the very fact of sound modification, are presented, and a comparison of these ways is given in order to find the best of them.
**Keywords:** *sound wave, emotional message, emotion concealment.*

*Научное издание*

# Актуальные проблемы информационной безопасности

Сборник статей

Выпуск 1

Издается в авторской редакции
Компьютерная верстка *Е. Ю. Никитина*

---

Объем данных 3,64 Мб
Подписано к использованию 10.09.2024

---

Размещено в открытом доступе
на сайте www.psu.ru
в разделе НАУКА / Электронные публикации
и в электронной мультимедийной библиотеке ELiS

Управление издательской деятельности
Пермского государственного
национального исследовательского университета
614068, г. Пермь, ул. Букирева, 15